Universidade de Aveiro Departamento de
Electrónica, Telecomunicações e Informática,
2015

Marco Rafael
Tenrinho Oliveira

Mobilidade em Redes Veiculares com Conectividade Dinâmica e Balanceamento de Carga

Mobility in Vehicular Networks with Dynamic Connectivity and Load Balancing

Universidade de Aveiro 2015
Departamento de Electrónica, Telecomunicações e Informática,

Marco Rafael Tenrinho Oliveira

Mobilidade em Redes Veiculares com Conectividade Dinâmica e Balanceamento de Carga

Mobility in Vehicular Networks with Dynamic Connectivity and Load Balancing

"The strongest of all warriors are these two — Time and Patience."
Leo Tolstoy

Universidade de Aveiro Departamento de
Electrónica, Telecomunicações e Informática,
2015

Marco Rafael
Tenrinho Oliveira

Mobilidade em Redes Veiculares com Conectividade Dinâmica e Balanceamento de Carga

Mobility in Vehicular Networks with Dynamic Connectivity and Load Balancing

Dissertaçao apresentada à Universidade de Aveiro para cumprimento dos requesitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica da Professora Doutora Susana Sargento, Professora Associada com Agregação do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e co-orientação do Doutor Tiago Condeixa, Engenheiro de Sistemas na Veniam.

o júri / the jury

presidente / president — **Professor Doutor José Carlos da Silva Neves**
Professor Catedrático do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

vogais / examiners committee — **Prof. Doutora Susana Isabel Barreto de Miranda Sargento**
Professora Associada com Agregação do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro (orientador)

Prof. Doutor Pedro Nuno Miranda de Sousa
Professor Auxiliar na Universidade do Minho - Escola de Engenharia

Agradecimentos

Gostaria de começar por dar um grande agradecimento aos meus pais pelo esforço que fizeram em me dar esta oportunidade e por terem sempre confiado em mim e nas minhas capacidades. Também aos meus avós e restante família pelo apoio incondicional e pela força que me deram. Além disso, um especial agradecimento à Diana por me ter aturado durante todo este tempo, ao Rui Lameiro e Tiago Almeida pelo apoio e compreensão, e aos meus amigos mais chegados que sempre estiveram ao meu lado e me apoiaram e ajudaram quando precisei sendo o meu grande apoio ao longo desta jornada.
Gostava também de agradecer aos meus colegas do laboratório de redes, nomeadamente o Tiago Almeida, Gonçalo Gomes, André Martins, Gonçalo Pessoa, Bojan, Francisco Castro e Rúben Oliveira pela força e alegria que sempre me deram, pelas alegrias e frustrações que partilhámos, pelas ajudas e apoio durante as fases mais complicadas e porque daqui sai uma nova família. Sem vocês seria muito mais difícil.
Gostava também de agradecer ao grupo de investigação NAP que sempre me ajudou quando precisei, destacando o Nelson Capela que me apoiou incondicionalmente e esteve sempre lá e a Professora Susana Sargento, minha orientadora, que me cativou e motivou nesta dissertação.
Todos vós foram um grande apoio e sem vocês não estaria aqui agora.
Obrigado por tudo!

Resumo

Com a evolução da tecnologia e da mentalidade do público em geral, cada vez mais os avanços tecnológicos levam à chamada internet das coisas e, por sua vez, a internet das coisas leva à criação de novos objetivos e à utilização de novas abordagens no que diz respeito às redes de acesso. Além dessa evolução, deseja-se também a comunicação estável e independentemente da tecnologia de acesso. Atualmente torna-se cada vez mais importante estar ligado em todo lado e a toda a hora, independentemente das condições de acesso.

A utilização das redes veiculares é cada vez mais uma realidade, sendo estas já utilizadas com vários objetivos e fornecendo variados serviços. Neste sentido, este tipo de redes já podem fornecer atualmente vários serviços à comunidade, nomeadamente a ligação à internet dentro do veículo, a recolha e utilização de dados sobre a cidade e, quando a utilização for estendida a veículos de utilizadores comuns, será possível o suporte para a segurança rodoviária e até condução autónoma.

Com a dinamicidade destas redes é comum um nó estar ao alcance de mais do que um ponto de acesso, mas quando isso acontece, apenas se liga a um deles independentemente da boa qualidade de ambos. Além disso, com a grande mobilidade dos nós da rede, a quantidade de alterações relativas ao ponto de acesso à rede é bastante grande, o que leva à extrema importância de garantir sempre uma boa ligação e uma rápida alteração da ligação sempre que necessário.

Esta dissertação concentra-se na necessidade de garantir a ligação simultânea a vários pontos de acesso à rede e uma rápida mobilidade dos nós de uma forma transparente para o utilizador. Com este objetivo, é realizada a integração do protocolo de mobilidade de rede Network PMIPv6 (N-PMIPv6) com uma extensão de suporte ao multihoming para o Proxy Mobile IPv6 (PMIPv6). Nesta integração as várias entidades que suportam o multihoming são integradas e adaptadas às características/ funcionamento do N-PMIPv6 de maneira a que estas estejam o mais adaptadas possível às condições das redes veiculares. É também utilizada uma particularidade da tecnologia veicular Wireless Access in Vehicular Environments (WAVE) para proceder a várias ligações com uma só interface. Além disso, o tráfego destinado aos utilizadores é distribuído tendo em conta as características das redes e do próprio tráfego. Relativamente às ligações efetuadas, a entidade de decisão e execução de ligações à rede é melhorada para permitir a ligação a vários pontos de acesso em simultâneo.

Por fim, obtém-se um protocolo de mobilidade para redes veiculares que suporta ligações simultâneas à rede, em que essas ligações são vistas e tratadas como pertencendo ao mesmo utilizador. Além disso, os testes de laboratório e estrada mostram que se consegue efetuar uma divisão do tráfego pelos vários caminhos minimizado o *delay*, maximizando a utilização de WAVE e minimizando os possíveis pacotes fora de ordem.

Abstract

With the evolution of technology and the demands of population, the technological advances are leading to the so called internet of things and, in its turn, the development of the internet of things leads to the creation of new objectives and to the utilization of new approaches regarding access networks. Besides, the stable communication is also desired independently of the access technology in use. Nowadays the importance of being connected always and everywhere is increasing, independently of the access conditions.

The usage of vehicular networks is getting to a reality, and they are used with several objectives and providing several services. In this way, this kind of networks can already provide services to the community like internet connection inside the vehicle, gather data from the city and, when the deployment extends to common users, some features like road safety and autonomous driving will be possible.

With the dynamicity of these networks it is usual that one node is in reach of more than one access point, but when this happens, that node will just connect to one of them independently of the good quality of those access points. Besides, with the high mobility of the nodes in the network, the amount of changes in the way the network is connected is high, which leads to the importance of having always a good connection and a fast change between networks when needed.

This dissertation focuses on the need to guarantee that one node connects simultaneously to several access points to the network and providing fast mobility of the nodes in a transparent manner to the users. Therefore, the integration between the N-PMIPv6 mobility protocol and a PMIPv6 multihoming support extension is performed. Several entities that support multihoming are integrated and adapted to the characteristics/operation of N-PMIPv6 in the way that they are as adapted as possible to the vehicular conditions. Also, a particularity of the WAVE vehicular technology is used so that one interface can connect to more than one access point at the same time. Besides, the traffic to the users is distributed in such a way that it accounts for the characteristics of the networks and of that same traffic. Regarding the connections performed, the entity that manages them is improved so that it can support more than one at the same time.

Finally, a mobility protocol for vehicular networks is obtained that supports simultaneous connections to the network, in which those connections can be seen and treated as belonging to the same user. Besides, the laboratory and road tests show that a division of the traffic through the several paths is performed in a way that it minimizes delay, maximizes the utilization of WAVE and minimizes the possible out-of-order packets.

Contents

List of Figures

List of Tables

Acronyms

16QAM	16 Quadrature Amplitude Modulation
AP	Access Point
AR	Access Router
ASU	Anchor Set Update
ASA	Anchor Set Acknowlegement
AT	Achieved Throughput
BA	Binding Acknowledgement
BCE	Binding Cache Entry
BC	Binding Cache
BSS	Base Station Subsystem
BU	Binding Update
CCH	Control Channel
CN	Correspondent Node
CoA	Care of Address
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
D-ITG	Distributed Internet Traffic Generator
DMIPA	Dynamic Mobile IP Anchoring
DNS	Domain Name System
DOT	U.S. Department Of Transportation

DSRC	Dedicated Short Range Communications
EID	Endpoint ID
ETR	Egress Tunnel Router
EUI-64	Extended Unique Identifier 64-bit
FCE	Flow Cache Entry
FDMA	Frequency Division Multiple Access
FM	Flow Manager
FN	Fixed Node
GPS	Global Positioning System
HA	Home Agent
HIP	Host Identity Protocol
HIT	Host Identity Tag
ICMPv6	Internet Control Message Protocol version 6
IEEE	Institute of Electrical and Electronics Engineers
IM	Information Manager
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol Version 6
ITR	Ingress Tunnel Router
ITSA	Intelligent Transportation Society of America
IVHS	Intelligent Vehicle Highway Systems
LISP	Locator/ID Separation Protocol
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MAC	Medium Access Control
MAG	Mobile Access Gateway

MANET	Mobile Ad-hoc Network
MAR	Mobility Access Router
MH	Mobile Host
MIPv6	Mobility IPv6
MIP	Mobility IP
mMAG	mobile MAG
MNN	Mobile Network Node
MN	Mobile Node
mps	mean packet size
MPTCP	MultiPath TCP
MR	Mobile Router
NA	Neighbour Advertisement
NEMO-BS	Network Mobility Basic Support
NEMO	Network Mobility
NIS	Network Information Server
NS	Neighbour Solicitation
N-PMIPv6	Network PMIPv6
OAI	Open Air Interface
OBU	On Board Unit
OFDM	Orthogonal Frequency-Division Multiplexing
OSI	Open Systems Interconnection
OS	Operating System
PBA	Proxy Binding Acknowledgement
PBU	Proxy Binding Update
PHY	Physical
PMIPv6	Proxy Mobile IPv6

PoA	Point-of-Attachment
pps	packets per second
QoS	Quality of Service
RA	Router Advertisement
RLOC	Routing Locator
RSSI	Received Signal Strength Indication
RSU	Road Side Unit
RS	Router Solicitation
SBC	Single Board Computer
SCH	Service Channel
SCTP	Stream Control Transmission Protocol
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TM	Terminal Manager
UCE	User Cache Entry
UDP	User Datagram Protocol
UIS	User Information Server
ULIT	Upper Layer Identifier
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USAGI	Universal playground for IPv6
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
VANET	Vehicular Ad-hoc Network
WAVE	Wireless Access in Vehicular Environments
WLAN	Wireless Local Area Network
WSMP	WAVE Short-Message Protocol

Chapter 1

Introduction

1.1 Motivation

Today, we live in a connected world and the tendency is to increase the span of access technologies to access the internet. In the last decade there has been a big increase in the number of connected users and in the number of devices per user. The trend is that each day we are witnessing a bigger growth than in the days before and looking at this evolution, one can expect that the trend is to have each time a more and more significant advance in the number and quality of the internet connectivity.

Nowadays, everyone is looking forward to being connected all the time and everywhere, without having to worry about different access points, different technologies or coverage. In this way, most of the devices that we use in our daily life are expected to be interconnected and supporting internet connection in the very near future.

Among these devices, one of the most promising are the vehicles, which can benefit in several ways with these connections. In this way the Vehicular Ad-hoc Networks (VANETs) come to accomplish this task of having several vehicles connected between each other and to the infrastructure that can provide internet connection. This approach allows the occupants of the vehicle to have access to the data that can be exchanged and take advantage of its applications, that can be related with many areas such as road safety, traffic management or comfort and media.

A VANET can be a reliable source of information and each area mentioned before can give way to important applications. In the case of road safety, this information can be used to prevent accidents by monitoring the relative position of each vehicle. On the other side, relating to traffic management, the network can be used to monitor the traffic state in each road and forward that information to the vehicles that can take a different path before it arrives to a more congested area. Furthermore, the comfort and media can be really important in this kind of technology, since it is in many cases the feature that is most appealing to the users. This last topic has a lot of room in this kind of network allowing several applications such as games between users of two different vehicles and internet connection wherever we go. Also, the evolution in this field takes us to wonder that with this, self driving cars would be also possible.

This concept of a VANET takes into account that every vehicle acting as a node of the network caries around an On Board Unit (OBU) that communicates with other OBUs in vehicles and with Road Side Units (RSUs) placed alongside the road, through WAVE technology (based on Institute of Electrical and Electronics Engineers (IEEE) 802.11p [1]). Besides this, OBUs can also communicate with Wi-Fi hotspots (IEEE 802.11 a/b/g) and cellular base stations (Long Term Evolution (LTE) – 4G). Moreover, the OBUs can provide a Wi-Fi access point to the users in the vehicles.

With the application of VANETs a big accomplishment is at our reach: being always connected. In this case, a vehicle can provide a connection every time. But with a dynamic network such as the VANET, an additional element is needed: a mobility protocol that maintains the connection while moving.

This mobility protocol has to be able to provide easy and fast handover allowing the user to maintain its connection even if he is moving at high speeds. Therefore, the vehicle needs to keep its Internet Protocol (IP) address so that the users will not need to restart their connection when they handover from one access point to another. In this aspect there are some mobility protocols that have been tested and improved in vehicular networks in our group.

In [2] and [3] it was proven that it is possible to implement a mobility protocol in vehicular networks with PMIPv6 and using WAVE technology. In [4] an improvement was made to this protocol providing mobility to the whole network, providing support for chains of vehicles and extending the coverage of the RSUs link constituting N-PMIPv6, that can use Wi-Fi, WAVE and cellular to connect. Besides this implementation, there were also implemented two more mobility protocols that were arranged and tested with vehicular networks and the technology IEEE 802.11p. These protocols, in contradiction to PMIPv6, were more distributed: one is a pure distributed protocol (Dynamic Mobile IP Anchoring (DMIPA) [49]) and the other is an hybrid Locator/ID Separation Protocol (LISP) [6]). Nevertheless, the N-PMIPv6 seems the most adequate, since it is faster and it implements network mobility.

Besides the mobility, there is another aspect that can help the user having a good Quality of Service (QoS) and seems like the next step in improving the protocols. Many times, a moving node is in reach of more than one Point-of-Attachment (PoA), and can benefit from this fact connecting to several PoAs at the same time. This behaviour is referred to as multihoming, and allows one user to be connected to two or more PoA at the same time, and send information through both, in a way that this user is seen as the same one by the network independently of the Access Point (AP) from which the information is sent. In our group a work is developed in this area that can be found in [7] and implements a multihoming approach using single-hop Wi-Fi and cellular technologies in a laboratory environment. This solution was built with the base of PMIPv6, one of the mobility protocols mentioned above, and it aims to minimize the mean time that the packets spend in the network through an analysis of the state of the access networks, the wireless characteristics and the traffic to each user.

In this way, a mobility protocol that supports multihomming is able to enable the complete support of all available access technologies in the road. As it is visible in the figure 1.1, the envisioned scenario includes single and multihop connections to several technologies, and some of the vehicles may take advantage of the several PoAs at range using, simultaneously, more than one connection (multihoming).

Figure 1.1: Desired scenario with possibility of multihoming and mulyihop

This dissertation motivation is to join together the mentioned N-PMIPv6 mobility protocol with the multihoming extension referred earlier. This will result in a vehicular mobility protocol with multihoming support which, to the best of our knowledge, does not exist with such characteristics or alike.

There are some challenges that need to be surpassed in order to have this solution, since the integration of the multihoming solution in the vehicular environment and with the N-PMIPv6 is not seamless. There are several aspects that need to be approached, namely the multihoming support in multihop scenarios, the utilization of the WAVE technology, the support for several connections of the vehicle at the same time, even with the same interface, and the adaptation of the multihomng processes to the dynamics of the vehicular environment.

1.2 Objectives and contributions

The needs of the actual VANETs go in the way that the QoS and reliability of the network are more and more important. Knowing with a good criteria how to divide the traffic is a key to evenly optimize the load of the network, and send the most time sensitive information through the paths that have a better quality. It is also important to adapt the solution to the characteristics of WAVE. This goes into the implementation of a multihoming approach to the VANETs environment, adjusting its features to this kind of networks and improving some entities so that the multihoming can be supported. In this way, this dissertation has the objectives listed below:

- Study the mobility protocols and their applications in VANETs
- Study the multihoming solutions and their possible implementations in VANETs
- Integrate a mobility protocol and a multihoming solution in a VANET scenario
- Use the characteristics of WAVE as an advantage of the multihoming solution
- Improve the connection manager so that it can connect to several networks at the same time, aiding with the support of multihoming
- Adapt the rule that distributes the multihoming traffic in order to better fit the characteristics of VANETs and its traffic
- Evaluate the solution in a real scenario

A first version of this work has already given way to a paper submitted in the 10th Conference on Telecommunications, Conftele 2015. Two papers are being prepared at this stage: one that considers the proposed multihoming connection manager and the optimal rule, and another that considers the overall solution and results in the road.

1.3 Document Organization

This dissertation is divided into several chapters:

- **Chapter 1 - Introduction:** The motivation objectives and contributions are clarified here.
- **Chapter 2 - State of the art:** This chapter summarizes the actual state and the most important features regarding VANETs, mobility and multihoming.
- **Chapter 3 - N-PMIPv6 and Multihoming - Concept:** Here, an overall review of the N-PMIPv6 and multihoming is performed. Moreover, the concept of this solution and its main operation is explained.
- **Chapter 4 - N-PMIPv6 and Multihoming - Implementation:** After the explanation about the solution in the previous chapter, the specification of more technical details is performed in an implementation point of view.
- **Chapter 5 - Evaluation:** The solution is tested and evaluated in order to verify the fulfilment of the objectives.

- **Chapter 6 - Conclusions and Future Work:** This final chapter concludes about the work performed and specifies possible future developments.

Chapter 2

State of the art

2.1 Introduction

In order to evaluate the extent of the work developed, it is important to understand the state of the technology and work that exists in this area. Therefore, this content will be explained in this chapter covering areas that extend from VANET's and mobility to multihoming. Regarding these topics, a list of this chapter's sections is described below:

- **Section 2.2 - Vehicular Networks:** This chapter gives an insight about what is a VANET, its main features, technologies and applications.
- **Section 2.3 - Mobility:** Here, the main mobility protocols are explained and their relations and application with VANETs are analysed.
- **Section 2.4 - Multihoming:** In the multihoming chapter an analysis is performed relating its features and challenges. Also, some solutions are analysed.
- **Section 2.5 - Chapter Considerations:** This final chapter analyses the addressed topics and provides the considerations about the work to be performed beyond the state of the art.

2.2 Vehicular Networks

A VANET is, as the name says, a network where the vehicles represent the nodes, and it is a particular class of a Mobile Ad-hoc Network (MANET). In this kind of network the vehicles are interconnected in an ad-hoc way and can communicate through several technologies such as Wi-Fi, WAVE or cellular, using an OBU in the vehicle that has the capability to communicate with other OBUs, and can also provide services to the vehicle occupants. As the network composed only by vehicles is very dynamic and is susceptible to loss of connection in some points, this network can also use RSUs placed alongside the road

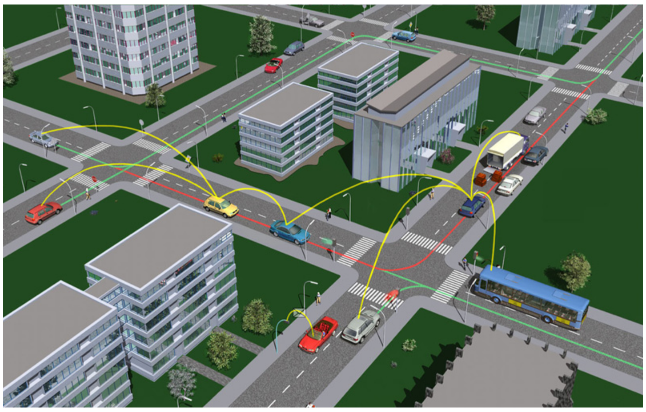


Figure 2.1: VANET city scenario [8]

to help keep the connectivity and also provide access to the Internet through a backbone to which these RSUs are connected. In figure 2.1 we can see an example of a VANET.

As the inter-communication and internet connection are becoming more and more an essential resource in our society, in the last years there was a big evolution in this area. This is related to the large amount of research and standardization that has been going on, allowing a large amount of entities involved in the research to have solid basis to work upon.

According to [9], the first step was made in 1991 when the United States congress attributed to the U.S. Department Of Transportation (DOT) the responsibility for a new program, the Intelligent Vehicle Highway Systems (IVHS) aiming to increase the safety of the roads, reduce pollution and conserve fossil fuels. By the year 1997 the involved parties in this evolution noted that the band between 902 MHz and 928 MHz was polluted and too small for the applications they aimed for. Consequently Intelligent Transportation Society of America (ITSA) asked for 75 MHz in the 5.9 GHz band with the goal of supporting Dedicated Short Range Communications (DSRC), obtaining it in 1999 as a spectrum between 5.85 GHz and 5.925 GHz.

In 2002 ITSA recommended that the same standard should be adopted for the Physical (PHY) and Medium Access Control (MAC) layers, achieving in 2004 the creation of the task group *p* of the IEEE 802.11 working group [10] that had the task of developing the amendments to the 802.11 standard so that it would include vehicular environments. The final draft was published in 2010 by this group and is known as IEEE 802.11p [1].

Meanwhile in Europe 70 Mhz were allocated also in the 5.9 Ghz band between 5.855 and 5.925 [1][11] with the aim to prevent road traffic and jams.

Also, in complementation with IEEE 802.11p and to create the WAVE protocol stack, the IEEE 1609 working group developed IEEE 1609 standards that cover the additional layers, namely, IEEE 1609.1 [12], IEEE 1609.2[13], IEEE 1609.3 [14] and IEEE 1609.4 [15]. This stack is now used in numerous projects in VANETs allowing an adequate communication between the nodes of the network.

Taking advantage of the communication Vehicle to Vehicle (V2V) (between OBUs) and

Vehicle to Infrastructure (V2I) (between OBUs and RSUs), in these networks each node can use their own data and the data received from other vehicles and infrastructures enabling the anticipation, detection and avoidance of undesired situations. In this way several services become available and can be used. These services provide not only an enhanced road safety and traffic management, but also comfort and media. These applications will be further explained in the section 2.2.2 of this document.

2.2.1 Features and Characteristics

The way VANETs behave implies that they constitute a new class of networks in which some intrinsic characteristics emerge. Some of these characteristics are beneficial and give certain advantages, but others are prejudicial and constitute problems that need to be dealt with. Next, some of the features of this kind of networks that make VANETs so special are listed [16][17][18]:

- **Nearly unlimited power and computation:** The fact that the nodes are vehicles enables he usage of the car battery and some of the available space. With this battery and space for bigger and potentially better components than in a normal MANET (e.g. antennas, memory, processor, etc...), there is the possibility of having powerful and effective OBUs that could allow a better communication.

- **GPS availability:** Vehicles travel in open roads allowing the possibility of Global Positioning System (GPS) usage to track and monitor the vehicle position and velocity.

- **Predictable movement:** With the mapping of information and the position obtained through GPS, the prediction of the next position of each node becomes possible. This prediction has to be a probability since the vehicle can change direction at any time.

- **High speed of the nodes:** The high speed of the vehicles (generally higher than 30 km/h) is a drawback and it makes the implementation in real world more difficult since the existent protocols and technologies are not prepared for high speed.

- **Dynamic network:** The nodes of the network have high mobility turning the network into a very dynamic one and with the possibility of creating separate clusters from time to time. Also, with this mobility there is a probability of disconnection of the node from the network when it moves to more unpopulated areas.

- **Hard analyses and experimentation:** The conventional network measurement tools like iperf [19] or ping are not prepared for such a dynamic environment, usually providing just end-to-end performance. In the case of VANETs, with dynamic multihop and multi-path connections, a complement to these tools is needed so that the characteristics like number of hops and path of the traffic is accounted for to cope with the dynamics of these networks.

- **Possible large scale:** With the evolution of the technology these networks need to be able to function in large scale scenarios as those will be the future, when hopefully all the vehicles can participate in one large connected network around the world.

2.2.2 Services and Applications

As said previously, a VANET has the possibility to accommodate a large range of services and applications going from safety applications to games and entertainment. Mainly, the applications in these networks can be divided in three different classes [20][21]:

- **Active road safety:** This type of application is usually low range and assists the driver helping with safety and reducing the probability of accidents and injuries to its occupants. If the vehicle has information about other vehicles in its surroundings and also about its own state, it can have the capability to prevent possible accidents. VANET applications can provide services like collisions warning and electronic brake, lane change assistance, overtaking vehicle warning, emergency vehicle warning or even signal violation warning like wrong way driving. Furthermore, complementing the direct road safety mechanisms, the self driving goal can be achieved with the use of all the information that is available to the vehicle. All this usability is considered of big importance and is extremely time sensitive, as it is given high priority. As an example, in figure 2.2 an accident can be avoided by broadcasting a breaking event to the ones behind.

- **Traffic efficiency and management applications:** The traffic related applications are normally network based and help with the general traffic flow, avoiding jams and increasing the quickness of the occupant's trip. This is accomplished by the processing of the information provided by the other OBUs so that the network can have the information about the state of the traffic. Also, in the management applications, the gathering of information about the city, the roads or the environment can be also performed. In these scenarios we can have applications like green light optimal speed advisory, ideal itinerary choice or even opportunistic garbage collection when the bins are full. The priority assigned to these services is lower than in the previous case, therefore not harming the time sensitive traffic.

- **User services and infotainment applications:** This kind of applications is normally used with access to the backbone of the network and to the internet through the RSUs and can bring a whole new world of entertainment and commodity services to the vehicle user. In this class it is covered the internet services, location related publicities or tourism informations. Contrarily to the previous cases, these services are the least important being therefore the least time sensitive applications.

Figure 2.2: Breaking event triggers the sending of a security message that warns the rear vehicles. Based on [22]

2.2.3 Access Technologies

Currently, there is a big range of access technologies that can be used in many different cases, but usually each technology is optimized to the scenario it was created or adapted for. Therefore, the choice for the most suitable one to apply in a VANET scenario needs to analyse some aspects. The most obvious choice is WAVE, but this is a relatively new technology, the deployment is scarce and takes time. In this way, some other highly deployed access technologies have to be taken into account.

In this section some of the VANET access technologies' characteristics are explained. It will be analysed, first, the native vehicular technologies DSRC/WAVE, and then, alternatives like Wi-Fi and Cellular. It will also be explained how one can use a multi-technology approach, and in what way these technologies bring benefits together.

2.2.3.1 DSRC

There are 75 MHz in the US and 70 MHz in Europe that are allocated to Dedicated Short Range Communications (DSRC) and are aimed to accommodate vehicle-to-vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. This portion of spectrum is allocated in the 5.9 GHz band and devises into seven channels of communication having each one 10 MHz as seen in figure 2.3.

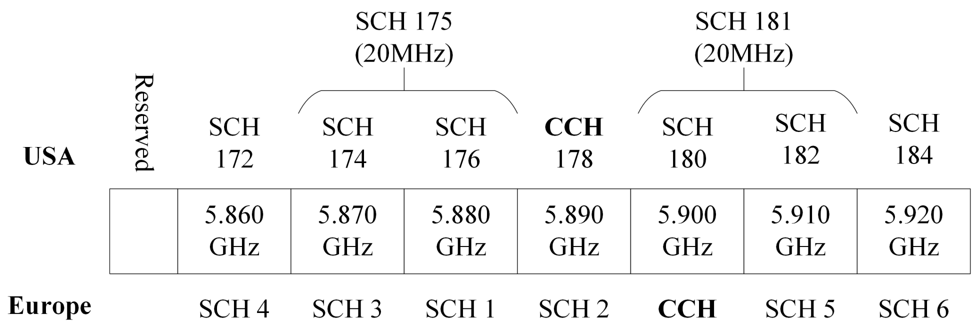


Figure 2.3: Channel allocation - USA vs Europe. Based on [11] and [18]

There are some differences in the allocated band between US and Europe, the main one is the channel usage. The applications aimed to the different channels are different and even the Control Channel (CCH) is in a different channel. Besides the channel differences, there are 5 MHz (5.850-5.855 GHz) that are reserved in US, and in Europe they are simply not allocated.

The different channels have different restrictions and aims as there is one CCH and the remaining six are Service Channels (SCHs). The main differences between these channels is that the CCH has a higher transmission power limit, and more benefits in the Time Division Multiple Access (TDMA). In the other side, some of the service channels can be grouped and be used as a 20 MHz channel so that higher rates are possible. These service channels are aimed to different uses such as road safety, future applications and non safety applications.

2.2.3.2 WAVE

Even though DSRC systems are used to improve the safety and the traffic flow, there is the capability of providing high-speed data services for the vehicle occupants, hence the creation of the WAVE standard was a big step in this evolution. This standard incorporates an amendment to the IEEE 802.11 standard and specifies the PHY and MAC protocols. WAVE systems operate in the 5.9 GHz band (5.850-5.925 GHz in US and 5.855-5.925 GHz in Europe) using Orthogonal Frequency-Division Multiplexing (OFDM) modulation that was adopted in order to reach data rates of 6 to 27 Mbs/s [23]. WAVE is built upon two standards that complement each other: IEEE 802.11p [1] and IEEE 1609.x family [12][13][14][15]. These standards define the WAVE Open Systems Interconnection (OSI) layers from 1 to 4 and will be further explained in this section.

WAVE communication stack

It is presented a simplified WAVE communication stack in the figure 2.4. WAVE supports two stacks which use the same physical and data-link layers and differ in the network and transport layers. These standards do not specify a session, presentation or application layers, but they do specify two more elements that do not fit well in the OSI model, which are the resource manager and the security services represented in the figure.

These stacks are the Internet Protocol Version 6 (IPv6) and a recent one exclusive to WAVE that is called WAVE Short-Message Protocol (WSMP). The reason for this is simple [9][24]: the first one will be used with traditional data exchange such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) constituting the so called data plane, and the second one will be used in high priority and time-sensitive communications. This allows the application to send time sensitive short messages with high priority, and at the same time, send the usual TCP or UDP messages.

IEEE 802.11p

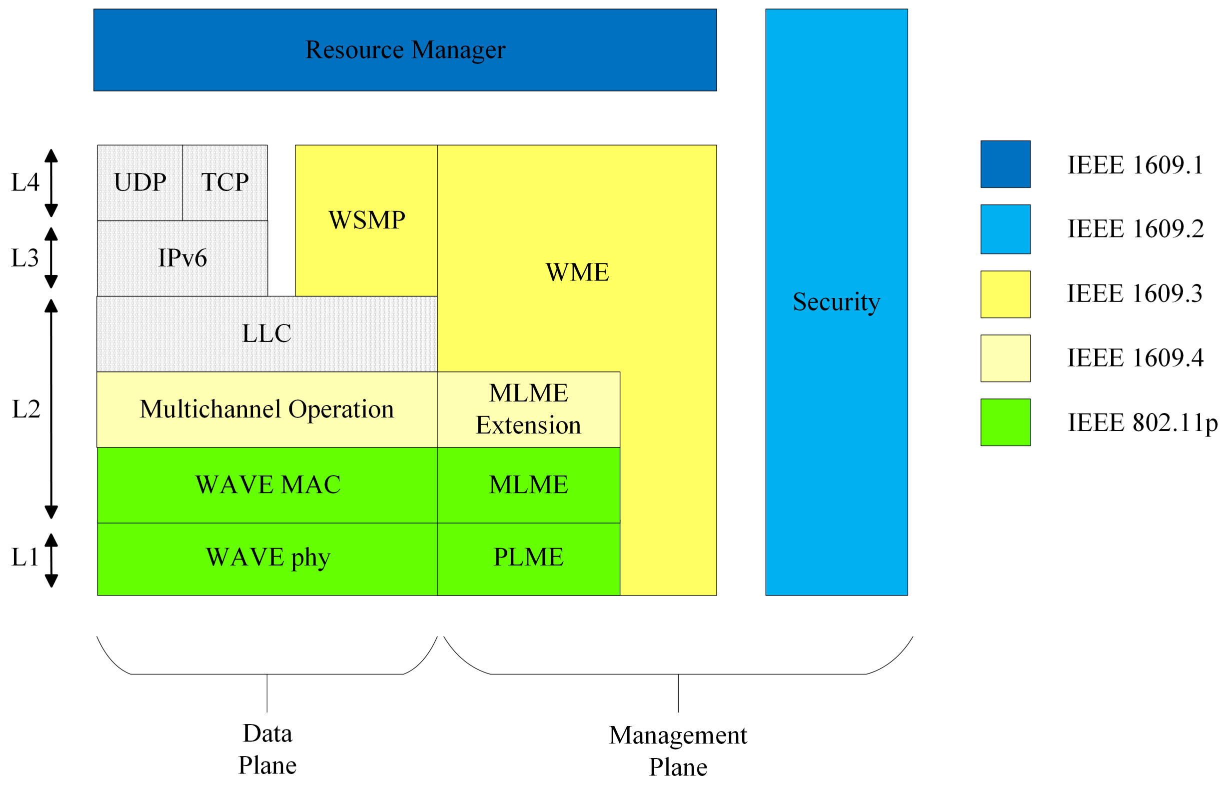


Figure 2.4: WAVE communication stack

IEEE 802.11p was designed to operate in the PHY and MAC layers and was specifically adapted from the IEEE 802.11 standards to work with the high mobile and volatile vehicular environment. Also, it supports the two different stacks that were mentioned in the previous section about WAVE stack (WSMP and IPv6).

It is OFDM-based, uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as a channel access mechanism[25] and is quite similar to the IEEE 802.11a physical layer from which it was adapted. The most important adaptations are listed below [23][26][9]:

- Longer ranges reaching up to 1 Km;
- Overal bandwidth of the channel goes from 20 MHz in IEEE 802.11a to 10 MHz in IEEE 802.11p which results in half the data rate;
- Utilization of seven channels in the 5.9 GHz band (one CCH and six SCH), same as in DSRC;
- High accuracy for the Received Signal Strength Indication (RSSI);
- 16 Quadrature Amplitude Modulation (16QAM) used in high mobility;

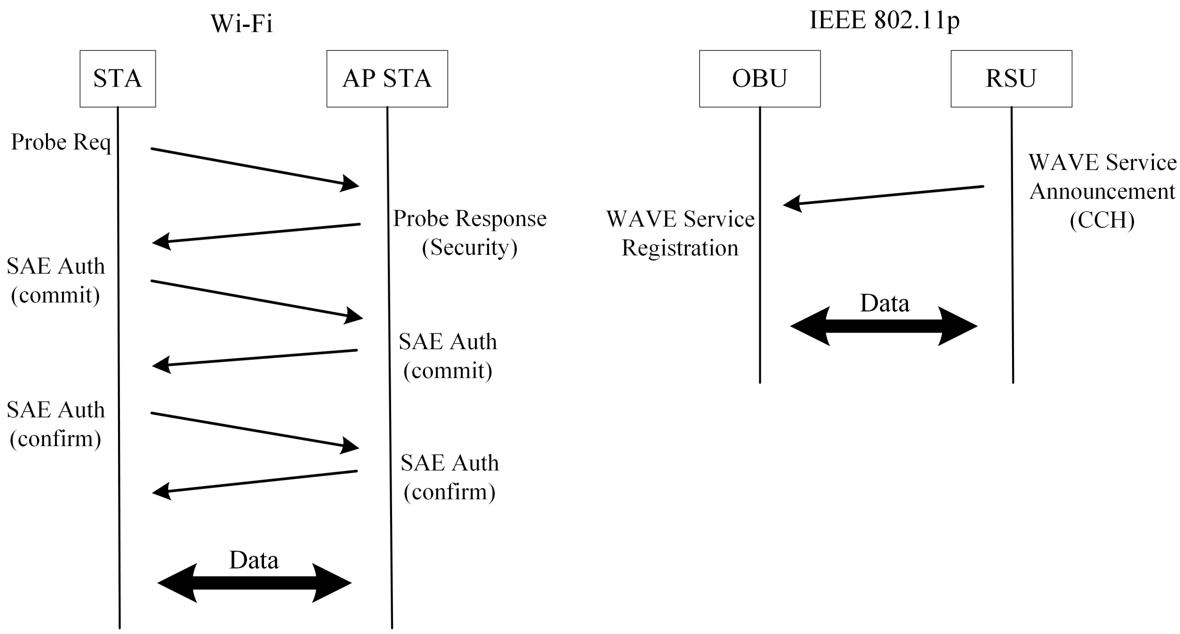


Figure 2.5: Messages exchanged: Regular Wi-Fi Vs IEEE 802.11p

- Power and priority control;
- Communication outside the context of a Base Station Subsystem (BSS).

One of the most important features of this standard is the operation in a high mobility environment. With the high mobility, the time of contact between two vehicles or between a vehicle and an infrastructure can be extremely reduced. This standard is defined in a way that exchanges data without the traditional association and authentication process allowing the node to communicate without having to wait for this process to end. Therefore, it results in a lower time until the exchange of useful information enabling the user to acquire more data in a smaller period of time. The figure 2.5 shows the enhancement made to the association process, and displays the messages exchanged when two nodes start the communication.

IEEE 1609.x

The IEEE 1609 family is composed by four standards that operate in layers two, three and four of the OSI model. These protocols are summarized below [27][20]:

- **IEEE 1609.4 [15]:** Enables the operation of upper layers across multiple channels without requiring the knowledge of the PHY parameters. It uses a TDMA and Frequency Division Multiple Access (FDMA) combination to deal with the multi-channel operation and specifies four modes of operation [28]:

- Continuous access, when the device works always in the CCH sending and receiving safety messages all the time.

- Alternating access is the default mode in which the device alternates periodically between CCH and SCH.

- Immediate access, when the device changes to the SCH right after the transmission in the CCH.

- Extended access, in which the device remains in the SCH more time than the periodic one when there is a big demand of non-safety messages transmission.

- **IEEE 1609.3 [14]:** Treats the WAVE connection setup and management, providing routing and addressing. It defines a management entity which is called WAVE Management Entity (WME) and specifies WSMP.
- **IEEE 1609.2 [13]:** Specifies the security concepts and message secure formats in order to have a safe communication.
- **IEEE 1609.1 [12]:** Corresponds to the resource manager that performs the interaction between the complex computing resources present outside the OBU and the ones within, so that the computation is seamless.

2.2.3.3 Combination of several technologies

Although WAVE is the obvious choice for the technology to use in VANETs, there is a problem: the deployment and consequently the coverage of the WAVE technology is still very small. Therefore, support for other technologies is needed so that the user has connection in all the roads he is travelling in. In order to do that, a multi-technology approach had to be followed taking advantage of the Wi-Fi hotspots that exist in many cities and of the cellular network that is deployed throughout most places. It will follow a small analysis to both these technologies through which we reach the conclusion that, although trying to be connected to WAVE every time, when it is not available we will try to connect through Wi-Fi and ultimately through cellular.

Taking these technologies, there are some aspects of each one that are needed to take into account:

- **Cellular** is a widely deployed technology that has passed through several structural and conceptual evolutions. The latest generations are Universal Mobile Telecommunications System (UMTS) which is known as 3G and LTE Advanced which is known as 4G, being the 5G still in a formulation phase.

  Regarding UMTS, an analysis in [29] concludes that in VANETs, UMTS could not guarantee the delivery of warning messages in time, being the latency twenty times bigger and the maximum throughput twenty times smaller than in IEEE 802.11 Wireless Local Area Network (WLAN) when regarding free channels in single-hop communication.

On the other side, it is feasible to implement a solution based on LTE and it may even compete with IEEE 802.11p beating it in some aspects, but being beaten in some others [30][31]:

- Coverage: LTE relies on the cellular network infrastructure which is widely deployed covering most of the territories.

- Market penetration: The penetration achieved by LTE is much bigger when compared to IEEE 802.11p, since the first one is already deployed in the devices used daily by the users.

- Capacity: LTE reaches 300 Mb/s downlink and 75 Mb/s uplink while IEEE 802.11p can only reach 27 Mb/s.

- Centralized architecture: Due to the centralized nature of LTE architecture, the direct communication V2V is not possible, since the messages have to pass through the infrastructure. This feature can influence the exchanging of safety messages in VANETs since it would easily overload the network.

- Status mode of the device: In most of LTE use cases, the resources are scarce and in order to save them, the terminals are kept idle when they are not being used. As the time necessary to switch states can be crucial, this feature can influence the performance of the network when time-sensitive messages are sent.

- High cost: The spectrum used in LTE communications is a licensed one, hence the communications may be charged. This takes a big cost when the communications are frequent, which would be the case.

- **Wi-Fi** is also a widely deployed technology, but in another way and with different characteristics. Traditional Wi-Fi is based on standards developed by IEEE 802.11 work group, and the better known to the public in general are the b, g and n standards, which are used in a major part of the electronic products that we use in the daily basis. These standards operate in the unlicensed 2.4 GHz band and can be affected by the interference of other devices using the same band.

  Wi-Fi hotspots that provide access to the internet are nowadays spread through buildings and streets of the entire world, but most of them are owned by someone that makes a regular payment to the operator for internet access. However, some cities provide free access hotspots to their inhabitants, and some operators have a network of hotspots that can provide free internet access to their subscribers when they are away from home.

  This technology can be used as VANETs access technology and it has some good and bad aspects when used in this kind of environments [32][33][34]:

  - It is widely deployed and consequently has a good coverage.

  - The wireless device is inexpensive allowing an easier deployment.

  - Some standards like IEEE 802.11n already support extremely high data rates.

- Contrarily to cellular, Wi-Fi can operate in two modes: centralized, when in communication with a PoA; ad-hoc, when in communication with another mobile node without using any infrastructure.

- Shows a low range, going up to just a few dozen meters which means that the high coverage mentioned before is a non constant coverage. This makes it necessary to be constantly connecting and disconnecting from different nodes.

- Has low support for mobility at high speeds, implying a session establishment in order to start to exchange useful data (as shown in figure 2.5) which is not a good aspect when regarding high speed nodes.

2.2.4 Architecture

VANETs are equipped with a series of particularities that make them unique. These networks should provide support for several types of applications and be able to execute every one of them in the best way possible. Besides, the network should also be able to support the high mobility and dynamics of the nodes. With this purpose, the architecture should be flexible and modular so that it would support applications with different complexities, allow the use of different communications frequencies, support different kinds of sensors and allow several types of control authority [35].

In this way, the nodes of the network should be able to communicate between each other, and can be classified as fixed or mobile (infrastructures and vehicles respectively). Taking this classification into account, the architecture can be classified in three different alternatives [18]:

- **Pure ad-hoc:** the network would be constituted only by vehicles operating in an ad-hoc manner, without the usage of a fixed infrastructure. This approach would allow the network to operate with just the OBUs placed inside the vehicles, but it would lead to a lot of clustering and would not allow a connection to a fixed network.

- **Fixed infrastructure with last hop wireless:** with this approach, the network would only rely on the fixed infrastructure deployed along the road for the communication between the nodes in a cellular manner. It can provide a good network once the infrastructure is deployed, but it would be dependent on it and communication between two nearby vehicles would be slower since it has to go through the infrastructure.

- **Hybrid:** the network would take advantage of the ad-hoc communication and of the deployed infrastructure, without relying on it, but using it to improve communication and reduce the clustering. The placing of the RSU infrastructure in strategic points of the road would allow the opportunistic communication directly or through another OBU in multihop. Figure 2.6 shows an example of this architecture which was proposed by C2C-CC [36].

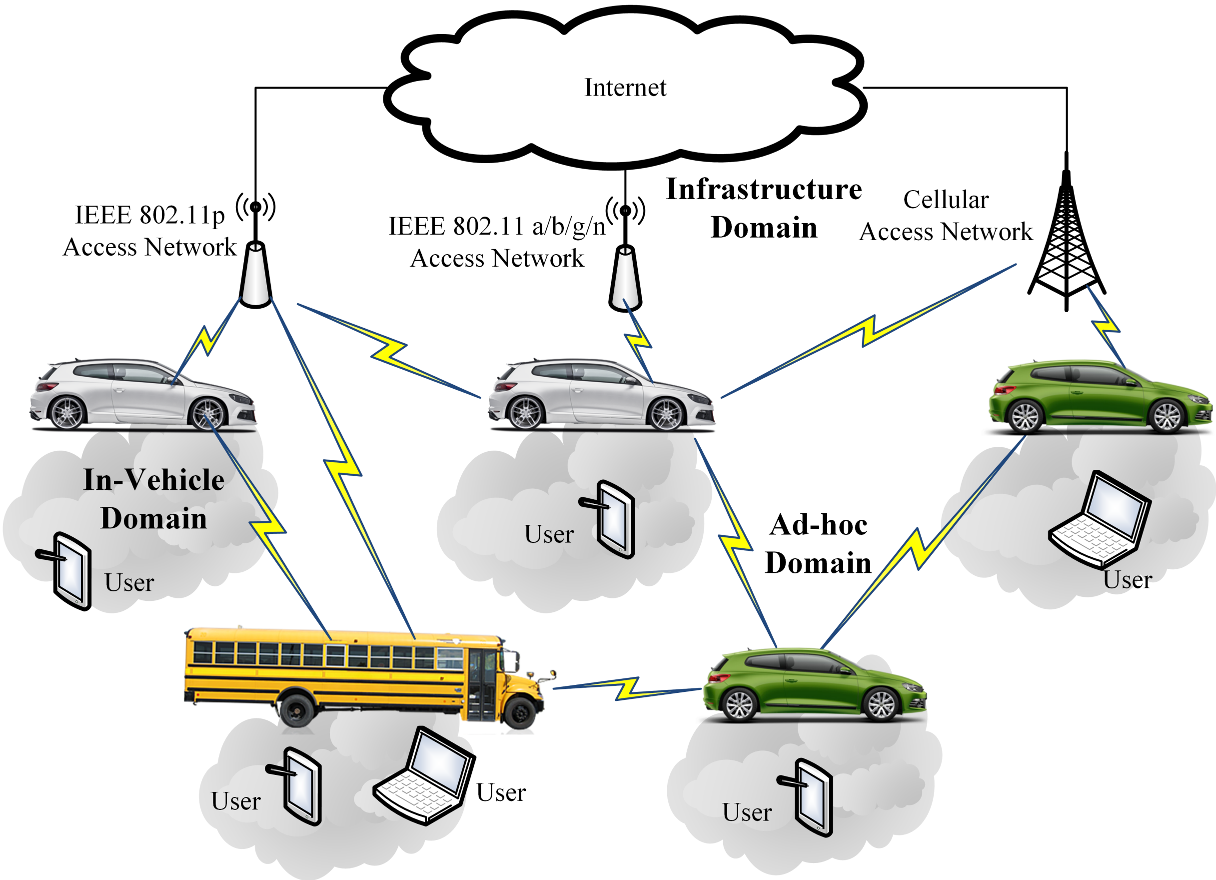


Figure 2.6: Architecture of a vehicular network, based on [36]

2.3 Mobility

The high mobility and increasing velocity of the vehicles makes the mobility management a crucial topic in VANETs. The connections must be seamless and provide continuous access to the users without them noticing any change. Therefore, there are some requirements and goals to be fulfilled [37][38]:

- **Seamless mobility:** The connectivity and service continuity should be guaranteed and independent of the vehicle whereabouts.

- **Fast vertical handover:** In order to achieve seamless service, this point is of extreme importance. Vertical handover allows the vehicle to roam between different access technologies, and fast handover allows the vehicle to improve the amount of time in which it is exchanging useful data, mainly noticed when the access points have a small coverage.

- **IPv6 support:** This support represents that the network will have a better security and QoS and also be capable to accommodate a big set of addresses.

- **Multihop communication support:** Multihop is apart of the VANET's reference architecture, so the mobility protocol should take that into account and be prepared to cope with it.

- **Scalability, efficiency and security:** The actual number of vehicles in the cities is quite big, so the scalability should always be an important matter and the networks should also be able to treat the mobility efficiently. Also, security problems should be taken into account so that the network can be reliable.

- **Multihoming support:** With the wide range of technologies and interfaces that may exist in the vehicle, multihoming support will provide the possibility to use more than one of those interfaces at the same time in order to take advantage of the available resources.

Furthermore, in infrastructured networks, the mobility management can be classified through several criteria [37]: network structure, user's roaming area, OSI layers or mobile host signalling. Although all of these criteria will be taken into account, the one further analysed in this case will be the last one, which distinguishes between host mobility and network mobility. In the case of host mobility management, it manages each vehicle individually. In the other side, network mobility management allows the vehicles to move as a group which improves the efficiency.

In this chapter some mobility management protocols are analysed and its operation is explained. This analysis will focus mainly on Mobility IPv6 (MIPv6), Network Mobility (NEMO), LISP and DMIPA related protocols which are the most interesting in the scope of this dissertation.

2.3.1 MIPv6

MIPv6 [39] is introduced as an improvement to Mobility IP (MIP) [40] using IPv6 instead of Internet Protocol version 4 (IPv4) and taking advantage of IPv6 mobility functionalities. MIPv6, as well as its ancestor, is a host mobility protocol that fulfils some of the mobility requirements mentioned in the beginning of this chapter, but fails to some of them, namely multihop and multihoming support.

The adoption of the IPv6 is easily explained: although MIP has been used for some time, the mobility between homogeneous and heterogeneous networks raises some problems that can not be handled by IPv4, like triangular routing, shortage of IPv4 addresses or security handling [41], and therefore a MIPv6 approach is more profitable.

2.3.1.1 Terminology

- **Mobile Node (MN):** Mobile entity such as laptops or mobile phones.

- **Correspondent Node (CN):** Fixed or mobile node that sends packets to the MN.

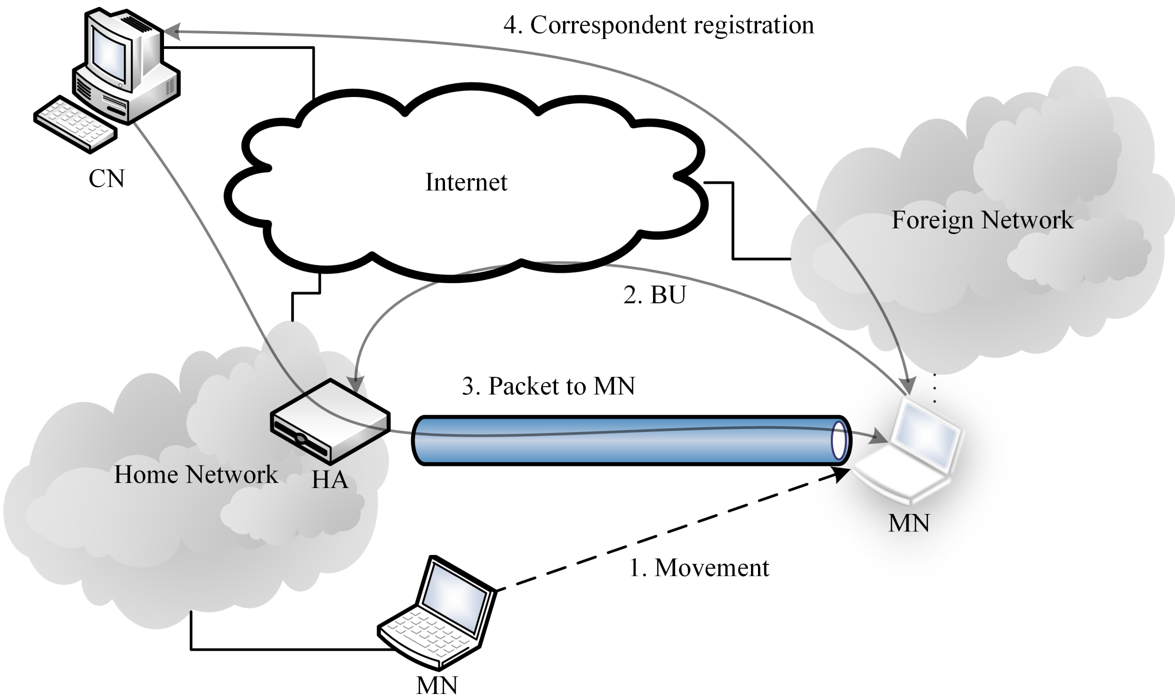


Figure 2.7: MIPv6 operation method

- **Home Agent (HA):** Existent entity in the MN's home network that contains its actual position. When the MN is not present in its home network, the HA intercepts the packets destined to the MN and tunnels it to its actual location.
- **Home network:** Network in which the mobile node resides primarily.
- **Foreign network:** Networks to which the MN connects to after it has moved.
- **Care of Address (CoA):** Address that the MN acquires when it roams to the foreign network.

2.3.1.2 Mobility management procedure

MIPv6 operation, shown in figure 2.7, is divided into four main steps:

1. **Movement:** the MN uses the IPv6 neighbour discovery protocol to detect its mobility from the home network to a foreign one, and it uses IPv6 auto-configuration mechanism in order to obtain a CoA.
2. **Update MN's information in HA:** After getting its CoA, the MN sends a Binding Update (BU) to its HA informing it about the CoA. The HA stores that information and responds with a Binding Acknowledgement (BA).

3. **Tunnel information to MN:** when the CN sends a packet to the MN, it gets to the home network and is intercepted by the HA. After that, it is tunnelled through a bidirectional tunnel created between the HA and the MN's CoA.

4. **Correspondent registration:** Finally, on receiving the encapsulated packet from the HA, the MN starts the process of the correspondent registration. This process will allow the CN with MIPv6 support to communicate directly to the CoA of the MN. If the CN has no mobility support, the two nodes will communicate through the existing tunnel between the HA and the MN, and then through direct connection between the HA and the CN.

2.3.2 NEMO-BS

Network Mobility Basic Support (NEMO-BS) [42][43] is an extension to MIPv6 that manages to support network mobility allowing the movement of a Mobile Router (MR) that is capable of providing a mobile network for several users to connect, and can also connect in multihop to another MR fulfilling multihop support. This extension creates NEMO-BS as a network mobility management protocol with multihop capabilities, but it still fails to provide multihoming support and also scalability, due to the increased tunnelling overhead.

This extension has the advantage to allow two types of nodes to connect to a MR: mobile or fixed ones. The fixed ones are always kept in the MR's network and roam with it, and the mobile ones can roam to a different network than the one of the present MR. When there is communication to the fixed nodes, only one tunnel is created to the CoA of the MR from its HA, but when the communication is to a mobile one that is connected to the mobile network, there is one more tunnel besides the one explained, through the existing one that goes directly to the mobile node from its own HA as shown in figure 2.8.

2.3.2.1 Terminology

The terminology used in this extension uses the MIPv6 terminology and introduces or alter some concepts:

- **MR:** This is a router that has the capability to change its point of attachment to the network and can also provide a mobile network that enables access to Mobile Network Nodes (MNNs).

- **MNN:** A node that has access through the mobile network. It can be classified as MN or Fixed Node (FN).

- **MN:** A node with the capability to change its point of attachment to the network. It can either be a Mobile Host (MH) when it has no forwarding capabilities, or a MR when it can forward data packets.

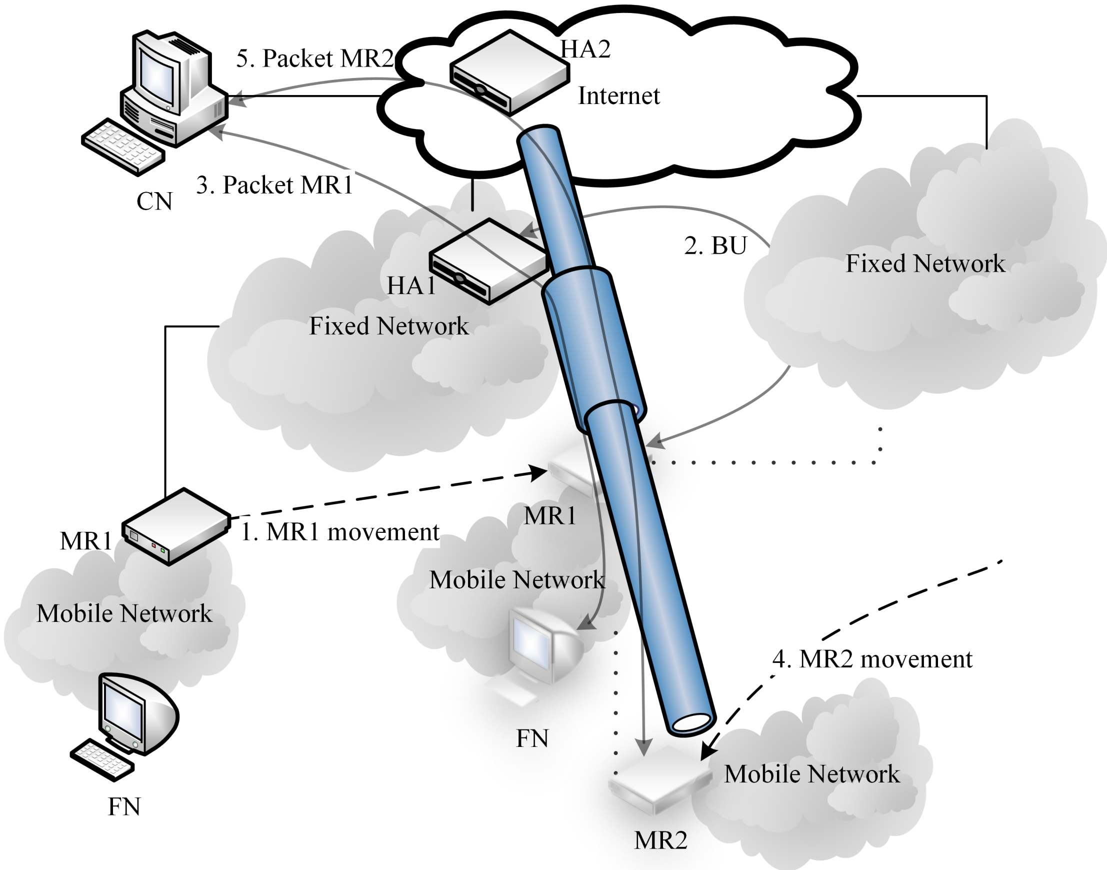


Figure 2.8: NEMO-BS operation method

- **FN:** A node without the capability to change its point of attachment without breaking the sessions.

2.3.2.2 Mobility management procedure

NEMO operation, shown in figure 2.8, can be divided into five main steps:

1. **Movement:** The MR uses the same mechanisms as in MIPv6 to detect the movement and acquire its CoA.

2. **Update MN's information in HA:** After acquiring its CoA, the MR sends a BU to its HA with the 'R' flag that indicates that it is a MR. It may also send the information of the mobile network prefix, so that its HA knows how to forward the packets destined to the MR's mobile network.

3. **Communication with a FN:** When a packet destined to a fixed node that resides in the MR's mobile network arrives to its HA, it is forwarded to the MR through a tunnel between its CoA and its HA, and once there, it is decapsulated and forwarded to its final destination. Upon that, the MR can keep the communication through the tunnel created to the HA or use route optimization as specified in MIPv6.

4. **Second MR movement:** When the second MR roams to the mobile network of the first one, it uses the same process as described before, but in this case, the communication passes through the already existent tunnel.

5. **Communication with a MN:** After the binding messages exchanged and the obtention of the CoA, when the CN tries to communicate with the MN, that is in this case the second MR, the communication is tunnelled through the second HA to the first HA and then through the first MR to the second MR.

2.3.3 PMIPv6

PMIPv6 [44] is a network based localized mobility management protocol that uses most of the functionalities introduced in MIPv6 and improves it in some aspects. This new improvements from MIPv6 are, according to [45], the elimination of the need to have mobility management functionalities in the user, its consequent effect on decreasing the overhead in the networks to which the MN is connected, and also the decreasing need to use MN resources such as processing and battery power. But, although this protocol solves some problems, it still fails to fulfil the previously mentioned requirements to a mobility protocol, and does not have multihop support neither distinguishes the several interfaces as belonging to the same user in multihoming.

2.3.3.1 Terminology

Apart from the MIPv6 terminology, PMIPv6 reuses some of it and introduces some more:

- **Local Mobility Anchor (LMA):** This new entity is basically an improved HA. It provides the MN prefixes, binds them and forwards its traffic;
- **Mobile Access Gateway (MAG):** Besides providing access to the MN, this entity also manages its mobility allowing an ordinary terminal to have mobility access;
- **Proxy Binding Update (PBU):** This type of message is a BU sent by the MAG and aimed to inform the LMA about a MN's binding information;
- **Proxy Binding Acknowledgement (PBA):** This message is a response to the PBU and aims to acknowledge the update reception and to inform the MAG about the prefix of the referred MN.

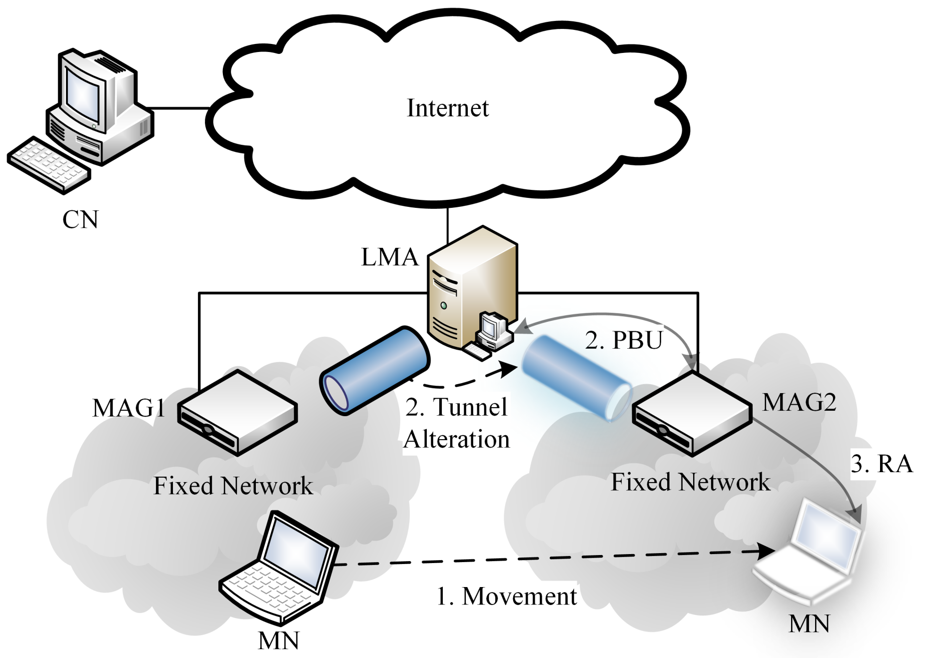


Figure 2.9: PMIPv6 operation method

2.3.3.2 Mobility management procedure

The operation method of this protocol is shown in figure 2.9 and is described as follows:

1. **Movement:** The MN uses the same mechanisms as in MIPv6 to detect the movement and tries to connect to the network by sending a Router Solicitation (RS) message.

2. **PBU and tunnelling:** Upon receiving a RS, the MAG sends a PBU to the LMA informing about the MN solicitation. When the LMA receives this message, it assigns the MN prefix sending it in the PBA and creating a tunnel to the MAG. Besides, if there are no more MNs in the MN's previous location, the previous tunnel is deleted.

3. **Router Advertisement (RA) with the MN prefix:** When the MAG receives the PBA, it sends a RA to the MN with its prefix.

2.3.4 N-PMIPv6

N-PMIPv6 [46] is an extension to PMIPv6 that enables it to support network mobility. As seen before, the network mobility allows a router to roam between APs without loosing connection and, at the same time, maintaining the users connected in its network. In N-PMIPv6 case, this router is called mobile MAG (mMAG) and is an extended version of the MAG of PMIPv6 that can recognize its own movement acting accordingly in order to maintain its connection. This protocol joins together the functionalities from

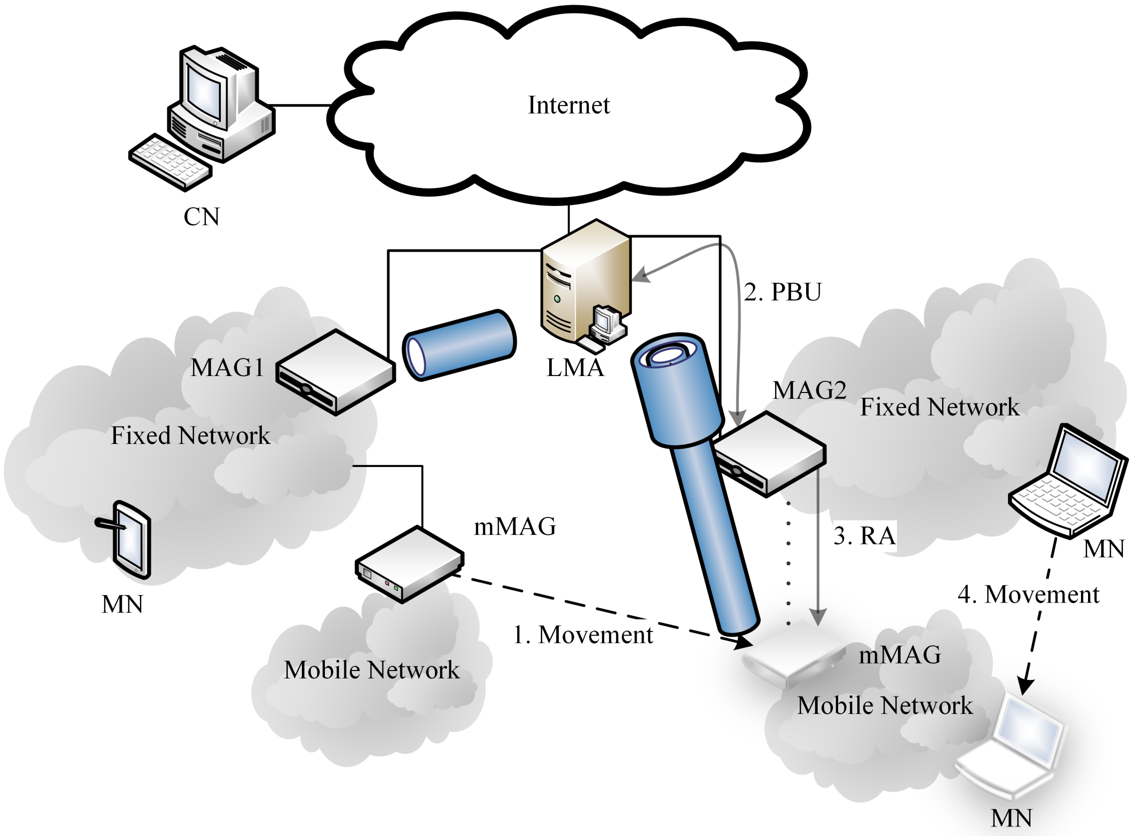


Figure 2.10: N-PMIPv6 operation method

NEMO-BS and PMIPv6, and manages to provide network mobility and multihop capability to PMIPv6, failing only to provide multihoming.

2.3.4.1 Terminology

The concepts used in N-PMIPv6 are the same as in PMIPv6 except for one introduced in this case:

- **mMAG:** This entity is a combination of the MAG in PMIPv6 and the MR in NEMO-BS. It is capable of providing access to the MNs in its network managing its mobility, and it also has the capability to change its own point of attachment.

2.3.4.2 Mobility management procedure

Figure 2.10 shows the method followed in N-PMIPv6 when a handover occurs. The method differs litle to the one used in PMIPv6:

1. **Movement:** The mMAG moves in the same way and uses the same mechanisms as the MN in PMIPv6.

2. **PBU and tunnelling:** Upon receiving a RS, the MAG or the mMAG to which it is connecting sends a PBU to the LMA informing about the mMAG attachment. When the LMA receives this message, it assigns the mMAG prefix sending it in the PBA and creating a tunnel to the MAG or mMAG to which the mMAG has connected. Besides, if there are no more MNs using the tunnel in the previous location, the previous tunnel is deleted.

3. **RA with the mMAG prefix:** When the MAG or mMAG receives the PBA, it sends a RA to the connecting mMAG with its prefix.

4. **MN roams to mobile network:** When a mobile node roams to a network provided by the mMAG, the usual and already explained process of authentication is performed, but with one change: the PBUs and PBAs sent between the mMAG and the LMA, have the 'M' flag set so that this communication is identified as relative to a node located in a mobile network.

2.3.4.3 N-PMIPv6 in VANETs

Considering the advantages of this protocol, its implementation was previously integrated in VANETs [4]. This N-PMIPv6 extension was adapted to work with WAVE/IEEE 802.11p technology which is somewhat different from the traditional Wi-Fi, since it does not have an association process and is broadcast-based. Besides, it was also integrated with a vehicular network manager that copes with the high mobility of the networks.

This approach is represented in the figure 2.11, and as we can see, the LMA is integrated in the backbone of the network communicating seamlessly with the MAGs which are integrated in the RSUs distributed alongside the road. On the other side, the mMAG is apart of the high mobility nodes that are the vehicles where the OBUs are placed. The mMAG takes advantage of the vehicular network manager to cope with the mobility triggering to perform the handovers.

There is currently a real testbed running in the city of Oporto that accounts with more than 400 vehicles and it uses a more distributed version of this protocol in order to increase the scalability and reduce the bottleneck effect. It uses more than one LMA in the network in a way that allows one node to be connected to the one selected by a selection server. This server listens to a request from the mMAG and replies with the LMA that the mMAG should connect to.

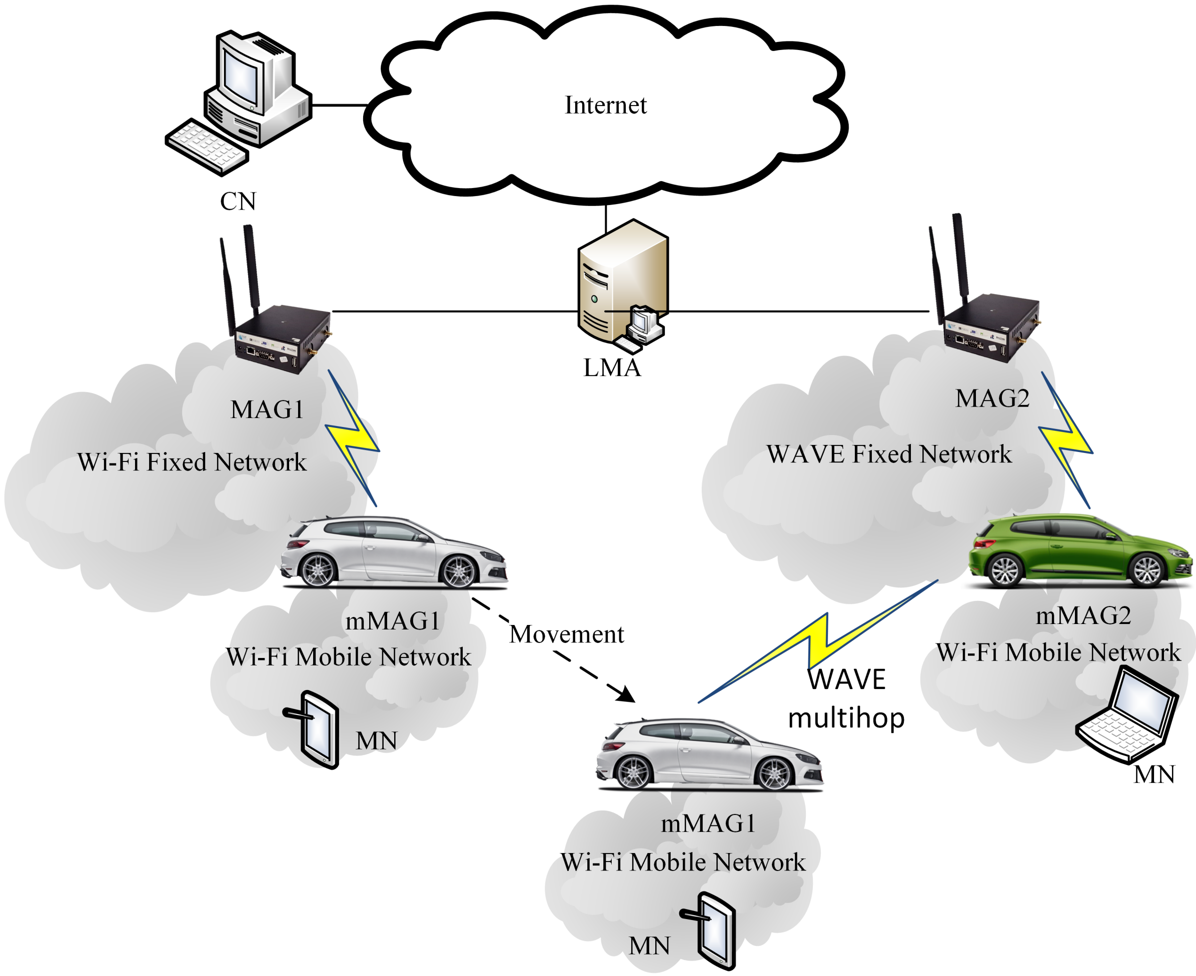


Figure 2.11: N-PMIPv6 in VANETs

2.3.5 LISP

LISP [47] is a protocol that completely differs from the ones previously presented here. It divides the traditional IP into two different namespaces: the Endpoint IDs (EIDs) and Routing Locators (RLOCs). The first one is used in the outer layers of the network, serves as an unique identifier for each node and is kept the same throughout the communication; and the second is used in the central part of the network and is used as a location identifier. To relate the EIDs and RLOC a distributed database is kept always updated. With this approach, the protocol can support multihoming just by keeping two RLOCs to the same EID in its database.

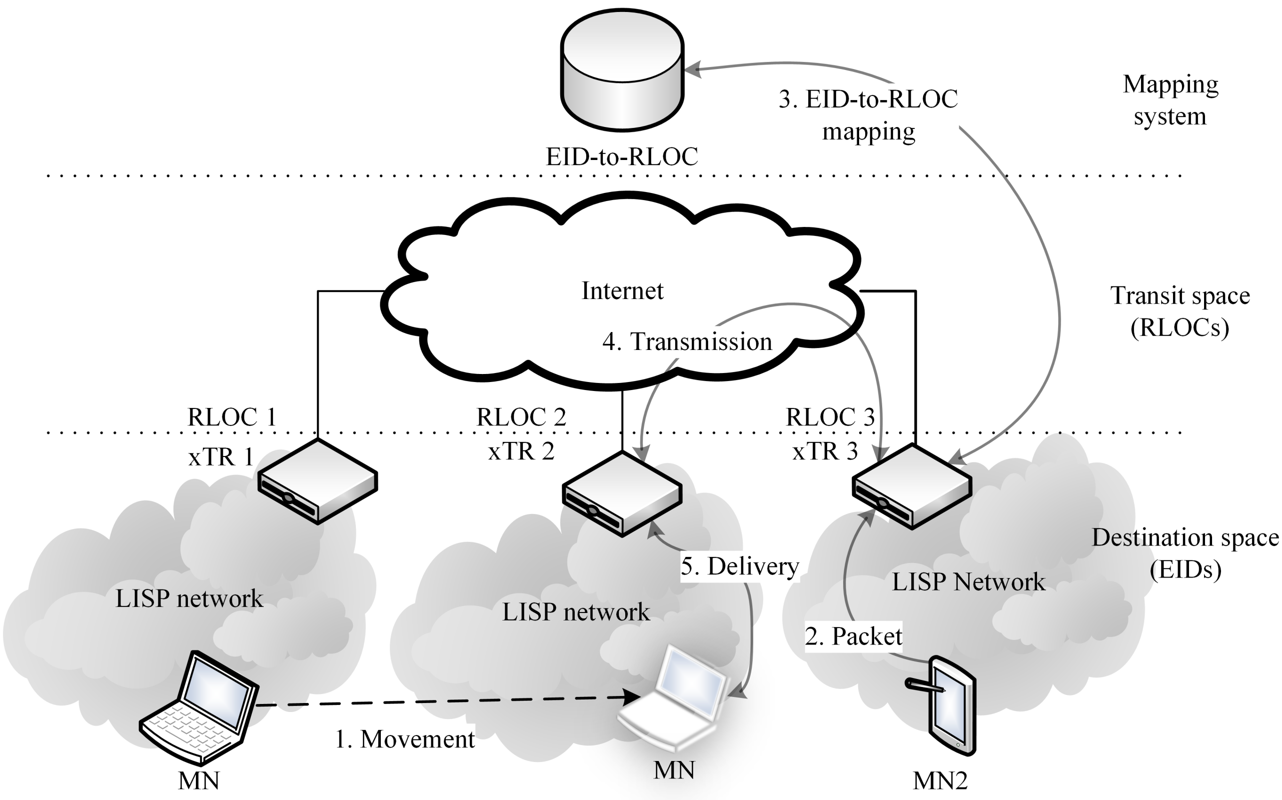


Figure 2.12: LISP operation method

2.3.5.1 Terminology

- **EID:** Is an IPv4 or IPv6 identifier that is used in the inner LISP header and identifies the end points of the communication.

- **RLOC:** Is an IPv4 or IPv6 address that belongs to an Egress Tunnel Router (ETR). One or more RLOCs can be used to map one EID.

- **Ingress Tunnel Router (ITR):** Is a router that receives packets from EIDs in a LISP site, performs the EID-to-RLOC mapping lookup and sends the packets encapsulated through the internet to the RLOC obtained.

- **ETR:** Is a router that receives encapsulated packets from the internet where the destination is one of its own RLOCs. It decapsulates it and sends it to the EID specified in the inner packet.

- **xTR:** Can be an ITR or ETR depending on the direction of the traffic flow;

- **EID-to-RLOC Database:** Distributed database that contains the information about the location of each EID.

2.3.5.2 Mobility management procedure

In LISP, the messaging is among the most crucial procedure. When a MN moves, the database is immediately refreshed with this new information, hence the most important feature here is how the communication is performed. These next steps can help with the interpretation of the figure 2.12:

1. **Movement:** When the MN connects to a new RLOC and the database is immediately updated.

2. **Communication starts:** the MN2 with its EID sends a message to the MN1 that goes firstly to the ITR.

3. **Mapping lookup and encapsulating:** ITR performs the EID-to-RLOC mapping lookup and encapsulates the packet to send.

4. **Transmission:** After receiving the information about the correspondent RLOC, the packet is sent through the Internet.

5. **Decapsulation and delivery:** ETR decapsulates the message received and delivers it to the respective EID.

2.3.6 DMIPA

DMIPA [48] [49] is a host-based distributed mobility protocol that uses a new architecture where the mobility is spread through all fixed PoAs and MN of the network. This protocol has some advantages in terms of scalability and deployability due to its tunnelling process and compatibility with legacy nodes. To reach the mentioned distributed mobility, DMIPA uses a dynamic anchoring strategy that allows one session to be anchored in any Access Router (AR) that has mobility support. This protocol provides a good scalability and performance, but still lacks multihoming and multihop support. Also, it will demand a good processing capacity of the machines used as RSU and OBU.

2.3.6.1 Terminology

- **AR:** Normal routers that do not support mobility.

- **MN:** Device that connects to the internet. It has an important role in the session continuity.

- **Mobility Access Router (MAR):** An AR with mobility features.

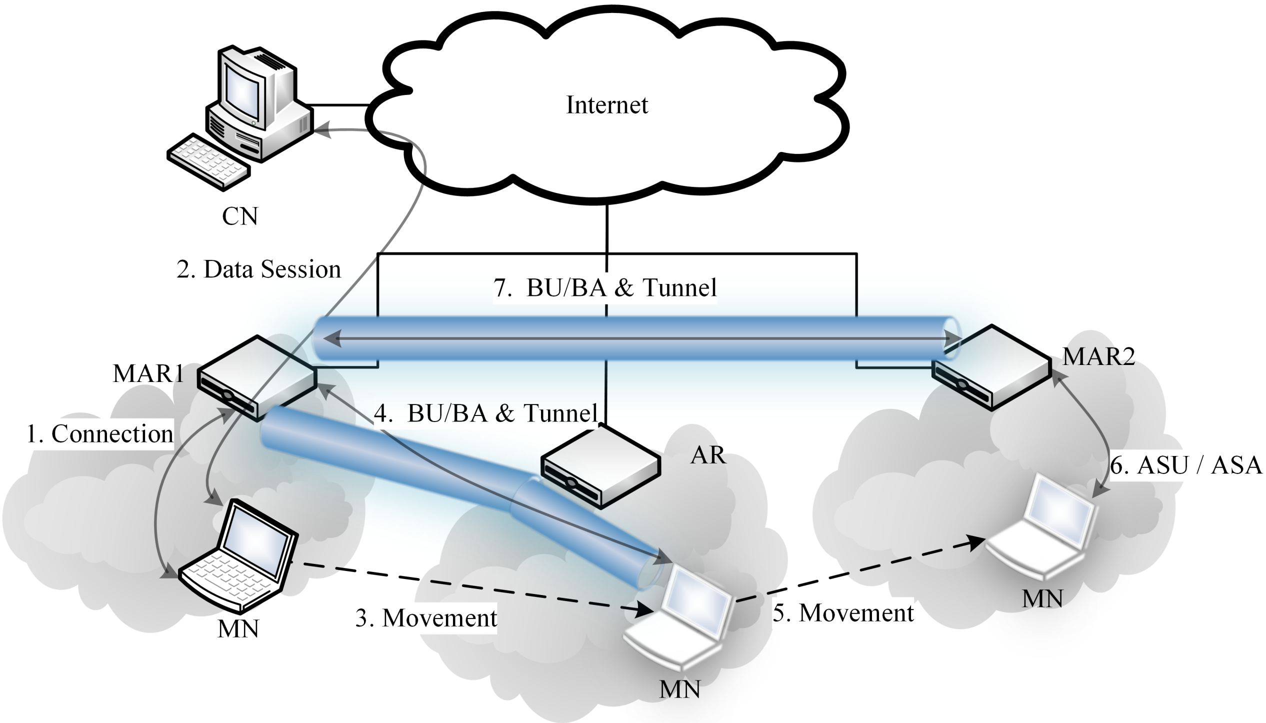


Figure 2.13: DMIPA operation method

2.3.6.2 Mobility management procedure

Figure 2.13 shows the normal mobility scenario of a MN from one MAR to an AR and to another MAR. This scenario helps to better understand the DMIPA operation [49]:

1. **First Connection:** The MN connects to the first MAR, configures its IPv6 address and adds this MAR's IPv6 to a database.

2. **Data session:** The MN initiates a data session.

3. **Movement:** The MN moves to the network provided by the AR, configures a new IPv6, but still keeps the previous one as the proffered address.

4. **Inform the actual anchor:** MN sends a BU to the MAR in order to establish a tunnel, and receives the confirmation in a BA. This will allow the aforementioned session to be tunnelled there from the MAR, and all the sesseions initiated in this configuration will be anchored in the mentioned MAR.

5. **Movement:** The MN roams to the second MAR's network to which it connects. The obtained address from this connection will be used as the new preferred address. Also, this MAR is added to the database of the MN.

6. **Anchor update:** MN informs the newly connected MAR about the other MAR and the set of IP used through a Anchor Set Update (ASU) message. In its turn, the second MAR acnowleges that message with a Anchor Set Acknowlegement (ASA).

7. **Tunnelling:** Second MAR sends a BU message to attempt the creation of a tunnel, and the first MAR acknowleges it through a BA message. A tunnel is then created between the MARs that supports the MN previously initiated sessions.

2.3.7 Considerations on mobility

Looking through the analysed protocols, some considerations can be made. First of all, relating to MIPv6, it is a widely used protocol nowadays, but it does not support multihop neither multihoming and is a host mobility protocol, which takes to a non desirability for its use in VANETs.

NEMO-BS eliminates one of MIPv6 main drawbacks which is the support for full network mobility and multihop. But, although it implements mobility for complete networks, it is not a very efficient protocol and presents very slow handover and registration times [50]. Therefore, it is not the most suitable one for a dynamic environment such as VANETs.

On the other side, PMIPv6 is a different extension of MIPv6. It allows the connection of users without the need of any special interaction in the MN side, and it has better performance than its ancestor MIPv6 [45], but it does not overcome the problems of the full network moility management, neither multihop or multihoming.

N-PMIPv6 extends PMIPv6 introducing the complete network mobility management and multihop support. Although it has some overhead due to the tunnelling system, this protocol fulfils the requirements to operate in VANETs. Besides, it was already implemented in the vehicular environment [4], and a more distributed version of it is currently working in a real testbed in the city of Oporto. Nevertheless, it still fails to fulfil the requirement of multihoming.

LISP takes a completely different approach from the ones analysed before, and accomplishes almost all the functionalities of a mobility protocol. But its method of operation has a big flaw that is the slowness of the access to the database when the location of an EID is needed. With this flaw, it is considered that LISP is also not suitable to work in such a dynamic environment as the VANETs.

Finally, DMIPA is a fully distributed protocol that brings the advantage of the easy scalability. It uses a strategy of dynamic anchoring to fulfil this, but its performance is not as good as the more centralized protocols like PMIPv6 or N-PMIPv6. Furthermore, it implies that the MAR and the MN have sufficient capabilities to manage the mobility when necessary. However, the distributed concepts of DMIPA have been implemented in a distribution of LMAs as it is running in the current Oporto mobility testebed.

Considering all these characteristics, the N-PMIPv6 protocol was the one adopted, so that it will be improved with multihoming support.

2.4 Multihoming

With the increasing interest in wireless networks and the continuous advancements in this area, the heterogeneity of the networks access technologies is increasing which leads to the increasing number of mobile devices that are equipped with multiple network interfaces. This scenario transports also to VANETs in which the multiple network interfaces are of most importance and where multihoming can bring a huge benefit.

Multihoming is defined as the ability communicate through multiple access networks simultaneously. This concept can be very important in VANETs because, besides enabling the increase of the network reliability, the bandwidth aggregation and load balancing, it can aid the mobility avoiding the loss of connection in handovers.

In this chapter, an analysis will be performed about the overall multihoming features along with the challenges and solutions of multihoming implementation.

2.4.1 Features

Multihoming can be divided into two different categories according to the multihomed entity. Namely, it can be performed at host or site level [51][52][53]. A multihomed host is one that uses two or more independent connections to edge networks; a multihomed site is one with two or more independent connections to the core network via multiple border routers or its interfaces. As an example, the multihomed host can be a smartphone, a computer or even a television or a fridge, while the multihomed site can be an enterprise or a campus network. Accordingly to the scope of this work, only the host multihoming will be addressed.

Multihoming solutions often aim to achieve some determined goals, which can be summarised, in most cases, through the following [54][55]:

- **Resilience:** This point can be obtained because the use of several paths to access the network allows the multihomed device to benefit from the other paths when one of them is lost. Also, the packet delivery ratio can be improved when there is more than one way to get to the end-point.

- **Ubiquity:** On a dynamic environment multihoming helps to maintain the connection ubiquity with the several paths. When one is lost, the communication is maintained through the others.

- **Load balancing/sharing:** This feature can be seen in two ways. The first one is that with several paths, the bandwidth can be improved when the traffic that would not fit through just one path, now fits through the aggregation of several paths. On the other side, the load balancing also allows the distribution of traffic to take into account the load of each path so that it evens the network load. Load balancing always has to take into account that the packet order can be affected, since the delay in each path can be different.

- **Flow distribution:** This feature combines all the previous ones and allows the flows to be distributed through the paths, and in the majority of the implementations multihoming allows not only the flows, but each packet to be relayed through multiple paths. This feature brings several benefits such as the cost reduction on increasing capacity, bandwidth optimization or bottleneck's effects optimization.

In order to implement multihoming solutions several setbacks need to be overtaken, such as the interface characteristic estimation, application characteristics, scheduling or network support and communication model. And also, depending on the layer of the multihoming approach, each one has its own challenges such as the extension of existent protocols in the transport layer or the congestion misprediction in the network layer (when using TCP traffic). These challenges will be further analysed in the next section and some solutions will be described afterwards.

2.4.2 Challenges

The implementation of multihoming solutions is often accompanied with some challenges that can be related to the mulhihoming per si or to that specific implementation. There are a set of challenges that are transversal to every solution [55][56][57]:

- **Interfaces characteristics estimation:** This is one of the most important points in multihoming operation. Each path to the end point needs to be carefully analysed so that the scheduling decision can be performed in the best way possible. There are several informations that need to be taken into account, such as traffic load, loss rate and interface capacity among others. This information can be directly measured or simply estimated.

- **Applications characteristics estimation:** In order to decide which traffic goes through which path, the characteristics of the traffic need to be known. This knowledge allows the scheduling to perform better decisions. This process can be performed by asking the applications what is the type of traffic or the bandwidth it requires or, in the other side, it can take a more compatible and transparent approach which is the estimation. Among the more usual estimation strategies are the ones that take as base the application name or the port it uses.

- **Scheduling:** Knowing how to direct the traffic is of most importance once there is more than one way to reach its destination. The problem here is not just where to direct it, but also how to do it. When it comes to where to direct the traffic, it can be performed in many different ways like round robin, maximum throughput, rate-based, energy and cost efficient among others. In the other hand, when it comes to how to direct the traffic, this can be done through packet-level scheduling or connection-level scheduling. The first one is the most used, and in this case the packets of the same connection can be directed through different paths leading to higher throughput. In the connection-level scheduling the packets of one connection go all through the same path.

- **Network support and communication model:** Different systems use different client-server communication models regarding to where the multihoming management is performed, so the support has to be adapted to each one. The three main models used are the updated-server-based that implements multihoming in the end-points (server and user), the proxy-based model that implements it in a proxy that is aware of the client's interfaces, and the legacy-server-based that implements it only in the users and maintains the servers and core network untouched.

- **Packet reordering:** When the packets of the same flow go through several paths that are characterized by different delays, the end point of the communication often receives them in a different order. This characteristic can affect the end-to-end delay because the reordering of the packets takes time and some real-time transmissions can be affected. Also with TCP connections, the out of order packets will be interpreted as lost and the transmission window will be shortened.

- **Battery power consumption:** Several interfaces mean that the terminal will consume more battery power, so the multihoming solution should take into account power consumption of the interface before it decides to use one more path. With VANETs, this point will not be important because the multihomed device is the vehicle, and it does not have power consumption constraints.

- **IP addresses location:** Every node is natively identified with IP addresses attributed to the interfaces, but the node does not have a location identifier, which constitutes a problem. Therefore, these IP addresses are used not only to identify the interface, but also its location. This can be a problem in the way that the routing is performed as a location based system, so the routing can not overcome the fact that one node is connected in several locations.

- **Sessions and flows are related to end point addresses:** The source and destination addresses can not be altered because this would cause problems in the identification of the flows and sessions. The same flows and sessions are bound to those edge IPs which is a problem because the different paths may still have the same source and destination IP. Hence, the differentiation may be a difficulty.

2.4.3 Solutions

To cope with the previously presented challenges, multiple multihoming solutions have been developed. These solutions are diverse and some are even implemented together with mobility solutions, since the mobility and multihoming are closely related to each other [57].

These solutions can be classified through multiple parameters such as its architecture, capabilities or others. Yet, the most common way is to classify according to the OSI layer that the solution that is implemented. Multihoming is usually implemented in one of these layers: MAC, network, transport and application layer. In the first case, the solutions are mainly used to communicate between two devices that are directly connected through more than one interface in order to achieve a better usage of the communication spectrum. Solutions implemented in the network layer continue to use the same transport layer protocols, operating only with the IP addresses and manage to communicate to interfaces of the same user with different IP addresses. In the other side, transport layer solutions are often implemented as a modification of the existent transport layer protocols such as TCP or UDP, or even as new ones. Lastly, the application layer solutions often manage to introduce an intermediate layer that may or may not oblige the application to support its extra operations. As they are the most accepted ones, next some network and transport layer solutions will be presented [51][52][54][57].

The identifier-locator technique is considered fundamental in multihoming and is used in the majority of the solutions. This technique can be implemented in different ways [51], namely the division of the IP addresses space in two parts or the usage of the first and last 8 bytes of the IP address separately. The first approach is often called map-n-encap and uses one set of addresses to provide the location of the nodes, and the other set to provide its identity. Furthermore, it implies the usage of a mapping system to relate both sets and implies an extra encapsulation that may be prejudicial. The second approach is often called 8+8 and uses the two parts of the IP in the same way, one for identification and another for location.

The first addressed solution here is Stream Control Transmission Protocol (SCTP) [58] which is a transport layer mechanism. SCTP defines a new transport protocol that has some similarities with TCP, but is still fairly different [59][60]. Starting by the different segments format, TCP implements a big packet header while SCTP uses a smaller header and groups pieces of data (chunks) with their own subheader that are sent beneath that main header. SCTP also supports multihoming, but it just uses paths other than the primary one to backup services. The secondary paths will be kept in a list of alternative paths and will only be used for retransmissions, or if the primary one permanently fails, which is not a full use of the multihoming potential.

Another transport layer solution is MultiPath TCP (MPTCP) [61][62]. This protocol extends TCP and enables it to use multiple paths to its destination node improving resource utilization and failure tolerance. MPTCP flows look just like normal TCP flows so that they can be backwards compatible. The communication starts just like a TCP connection, and then when there are more paths available, the MPTCP initiates sub-flows that take advantage of the multiple ways to reach the end-point.

LISP [47] on the other side is a solution already studied in this document in the mobility analysis. This solution uses the map-n-encap method and, with the two sets of addresses, it identifies the EIDs and the RLOCs. LISP needs a relatively fast and reliable mapping system that could cope with the necessities of the network. With the high mobility and dynamics of a VANET this can be of extreme difficulty, so this does not seem like a good solution to the VANET problem.

Relatively to Host Identity Protocol (HIP) [63], it uses an identifier-locator split in which the IP address is its locator and its identifier is a public part of a public-private key-par. The identifier is composed of an IPv6-like address that uses a special prefix called Orchid [64] and a 100 bits cryptographic hash. This identifier is called Host Identity Tag (HIT) and is used for addressing in the upper layers. With this approach, the Domain Name System (DNS) can be used as a resolution and mapping functionality, although it is not a fast alternative and not viable for mobility.

Shim6 [65][66] also uses the identifier-locator split, but in a different way. When the communication starts, it starts normally to one of the host's addresses, and in that moment that address becomes the identifier of the node until the communication is over. The remaining addresses of the node are from that point on seen as the locators and are used for routing. The identifier in this case is called Upper Layer Identifier (ULIT) and is very similar to the HIT in HIP, since the communication can be done through it in the upper layers also.

There is also a network layer multihoming solution developed in our research group that extends the PMIPv6 mobility protocol. This solution is presented in [7] and implements a proxy entity together with the PMIPv6's LMA. That entity manages all the multihoming processing and conceals the use of several paths from the server. This solution uses a dynamic connection and disconnection process, and uses IP replication in a controlled manner in the user side to enable the use of multiple paths when transmitting a certain flow. Moreover, it schedules the packets in the way that it minimizes the mean delay and takes into account several parameters for each path classification, such as achieved throughput, capacity variation and packet loss. Also, it uses the 8+8 system using the prefix of the IPv6 as an identifier of the node and the last 8 bytes as the locator.

Concluding, and taking into account all the multihoming solutions, the one that seems more suitable for VANETs is the extention of PMIPv6. It allows both mobility and multihoming in a reliable and fast manner, manages to do a good analysis of the networks and performs in a packet basis multihoming optimizing traffic division.

2.4.3.1 Proxy multihoming as a PMIPv6 extension

As this was the chosen solution, a further explanation will be performed. This solution is divided into three main segments: Core Network, Mobile Access Networks and End-Users Terminals.

Firstly, the Core Network contains the main entities that allow the multihoming in an intelligent and dynamic way. It contains the Terminal Manager (TM), Flow Manager (FM), Information Manager (IM) and PMIPv6.

Besides monitoring the terminal and its interfaces, the TM binds the several interfaces and its respective terminals. FM is used to manage the terminal's traffic and is able to recognize the binding of each data flow with its terminal. Moreover, it has the ability to recognize when the use of multihoming is profitable, calculates the traffic division rule and applies it to each packet. The IM, on the other side, manages to collect all the data used in the multihoming process. Lastly, the base entity is PMIPv6's LMA that is running on the Core Network to manage all the mobility.

In the Mobile Access Networks two entities operate in each access router: Network Information Server (NIS) and PMIPv6. The first one performs the necessary operations

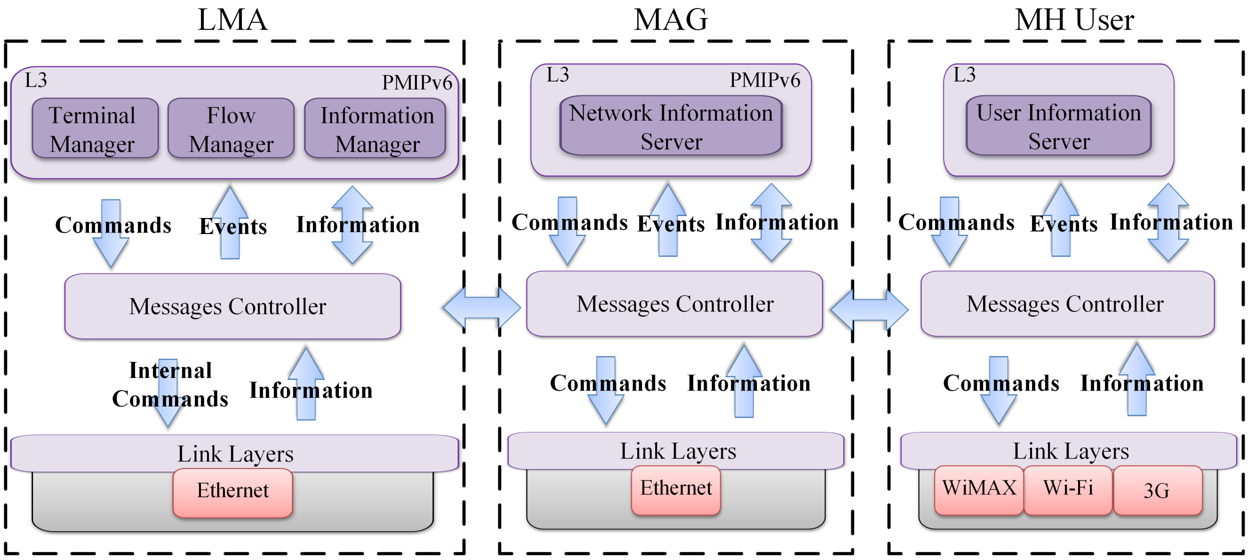


Figure 2.14: PMIPv6 extension multihoming framework [7]

to obtain and send the information about the access networks to the Core Network, and PMIPv6 operates here with its MAG entity.

In the case of the End-User Terminals, only an User Information Server (UIS) operates in order to provide information about its connection.

In the figure 2.14 we can see the framework of this solution, in which the multihoming and mobility entities are represented. The entities operate in layer 3 and communicate with each other through the link layer technologies represented in the image.

2.5 Chapter considerations

Analysing the addressed themes, a mobility and a multihoming solutions were selected to work upon taking into account the characteristics of the VANETs in which they will be implemented.

Starting with the VANETs, they are really dynamic networks that can be used with several applications that go from safety applications that avoid accidents, traffic management ones, comfort and media or even autonomous driving. This kind of networks can incorporate several technologies that allow the communications V2V and V2I.

Regarding the option about a mobility protocol to integrate with VANETs and multihoming, the chosen one was the N-PMIPv6 that had already been implemented and tested in a real vehicular scenario and implements a fast network mobility.

In the other side, regarding all the challenges and different solutions to the multihoming problem, from the analysed ones, the PMIPv6 extension was chosen to integrate with the chosen N-PMIPv6 mobility protocol. This solution has the advantage of being built from the same basis as the mobility protocol, and it also implements an intelligent traffic division based on the characteristics of the networks.

With this, the N-PMIPv6 mobility protocol and the multihoming extension for the PMIPv6 will be integrated in order to have a network mobility protocol with multihoming support.

Chapter 3

N-PMIPv6 and Multihoming Integration

3.1 Introduction

As explained in the previous chapter, mobility and multihoming are two very important areas in the VANETs. In one side, mobility will allow the users to roam through access points guaranteeing the sessions continuity; in the other side, the users with several network interfaces will be able to use them all within the same data session. In this way, the evolution of the technology requires a mobility protocol that supports multihoming. The chosen one that implements the mobility part was a PMIPv6 extension, the N-PMIPv6 as explained in the previous chapter. Regarding multihoming, the chosen solution was an extension for PMIPv6 that was already implemented and experimented in a single-hop wireless and cellular environment.

In this work, the aim is to implement and test a multihoming solution that can be used in a vehicular environment, and that can also profit from the network mobility provided by N-PMIPv6. This multihoming solution will be adapted from the referred PMIPv6 multihoming extension and will be extended to support a vehicular scenario. This work is developed in parallel with another dissertation work and focuses on some of the main aspects of the multihoming implementation:

- **Interaction of N-PMIPv6 and multihoming:** Although the multihoming solution and N-PMIPv6 were both developed with a PMIPv6 basis, they have some differences that need to be resolved. Also, the multihoming solution will be transported to different equipments which may bring different behaviours.

- **Multihoming with one IEEE 802.11p interface:** Sometimes one vehicle can be in the range of several other nodes that can provide connection to the network in single hop or multihop using the same VANET technology (WAVE). IEEE 802.11p used in WAVE is a broadcast based technology, and there is no session establishment like in the traditional Wi-Fi networks. This feature allows one node to communicate to two other nodes just by sending two different messages. In this way, one interface can be used to connect to two or more PoAs providing two or more paths to the rest of the network.

- **Multihoming connection manager:** The mobility protocol and multihoming operation are not possible if there is no entity available to change and maintain the connections. This entity needs to perform the connection and trigger the handover process. Although a simple mobility connection manager was developed in another dissertation, a more complex one is needed in order to implement the multihoming functionalities. The base connection manager implemented in the other dissertation was developed to support mobility, but it was built from the base up in order to be prepared for the multihoming implementation, with one processing flow per each interface and another to receive control packets. In this dissertation, the processes are optimized in order to support the simultaneous connections, taking advantage of the several interfaces, support the one interface multihoming mentioned in the previous point and manage the different connections. Upon this improvement, the support for cellular connection is implemented also in the parallel dissertation.

- **Mobility and multihoming rule:** The multihoming extension for PMIPv6 has already a mechanism that calculates the percentage of the traffic that should be transmitted through each path, according to its achieved throughput, capacity variation, networks load and packet loss. This division is performed in a per packet basis, but with the dynamics of VANETs, the delay difference between paths becomes more relevant and some paths can even disappear during a transmission. In this way, a qualitative classification of the different paths is performed. Moreover, both network and traffic characteristics change in the vehicular scenario and the multihoming rule needs to adapt to this new environment.

Considering the mentioned points, section 3.2 will explain the basic operation of the two solutions that are being integrated, and also explains the operation of the first stage integration; section 3.3 explains how it is possible to use multihoming with just one interface and its consequences; section 3.4 explains the operation of the multihoming connection manager; section 3.5 elucidates in what way was it is possible to adapt the traffic division rule in order to better distribute the traffic to the VANETs case; finally, the section 3.7 wraps everything together and gives an overview of the chapter.

3.2 Multihoming and N-PMIPv6 integration

The multihoming solution and the N-PMIPv6 are both PMIPv6 extensions, and were developed with the same basis: an available implementation by Open Air Interface (OAI) [67]. This implementation is based on the implementation USAGI-patched Mobile IPv6 for Linux (UMIP) [68] version 0.4 which, in its turn, is based on the Universal playground for IPv6 (USAGI) [69] version 0.4 implementation. The N-PMIPv6 version was already

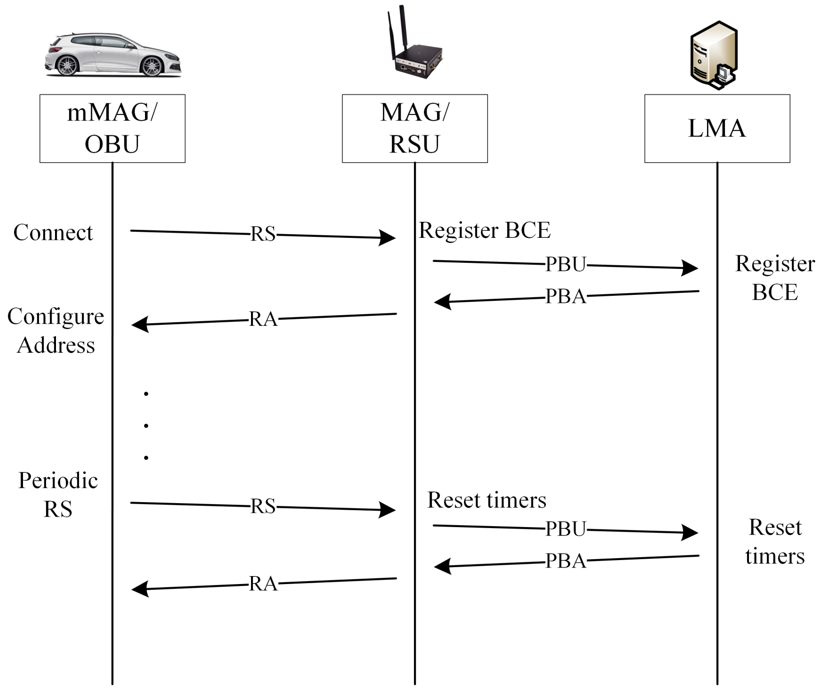


Figure 3.1: Representation of N-PMIPv6 control messages exchanged

modified in two dissertations that improved the mobility [3][2] and the network mobility [4] described in N-PMIPv6 [46]. On the other side, the multihoming extension was developed directly from that PMIPv6 base implementation by OAI and is an extensive solution that manages the user's interfaces and flows.

Understanding the essence of the approaches is essential to understand their combination, so in the next sections a further explanation of the N-PMIPv6 and multihoming implementations will be performed. Also, an explanation about the combination of both takes place after those sections.

3.2.1 Adapted N-PMIPv6 Operation

N-PMIPv6 was developed to run in a vehicular mobility management solution that enables OBUs placed in the vehicles to roam freely, maintaining its sessions active and maintaining also the sessions of the users inside the vehicle. The vehicles are constantly directly or indirectly (multihop) connected to a WAVE RSU that allows connection to the fixed network or to a hotspot Wi-Fi or Cellular base station. Moreover, this solution names three main entities: LMA, MAG and mMAG. These entities were already mentioned in the previous chapter.

The N-PMIPv6 solution that was used as a starting point was improved relatively to the one described in [4] and [70], namely, it has a better behaviour in the real network. The Neighbour Solicitation (NS) process used to verify the existence of the link layer address had been withdrawn from the process as a measure to lower the number of messages in the

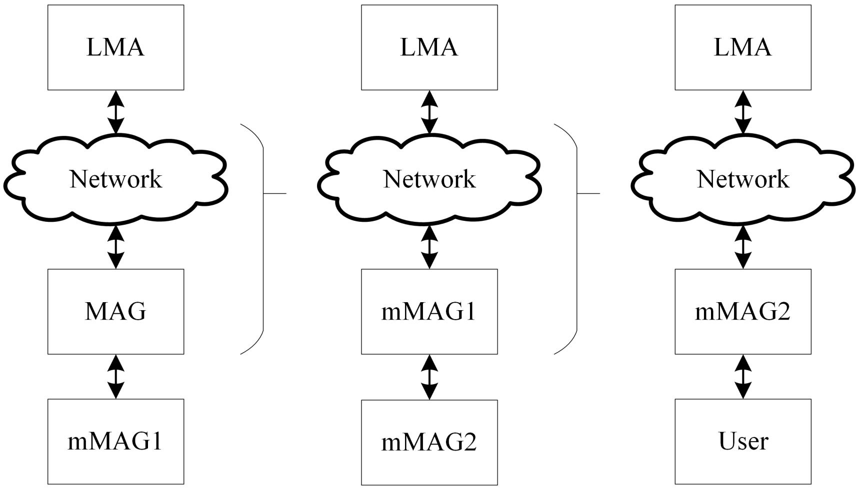


Figure 3.2: Network abstraction used in N-PMIPv6 that supports multihop, based on [70]

high dynamic environment of a VANET. With the dynamics of the network, the mMAG is constantly changing its PoA and also losing connection. With the new approach of sending periodic RSs to maintain connectivity, the mMAG does not need to fail in the neighbour discovery, it will just send a new RS to the best network at sight (although taking into account a hysteresis if there are two good networks at sight). Figure 3.1 represents a summary of the messages exchanged in the adopted N-PMIPv6 implementation.

With respect to the multihop operation of N-PMIPv6, this operates in a network abstraction manner. As depicted in the figure 3.2, the mMAG that connects to a PoA in the network always sees that PoA as a MAG even if it is another mMAG. In its side, the PoA operates as a MAG to the nodes that are connecting to it, and operates as a user to the nodes that are providing the connection.

In the figure 3.3 it is visible an overall scheme of the N-PMIPv6 operation in the registration and mobility management of the nodes. Note that another mMAG or a user can connect to the mMAG.

The operation is only triggered when the mMAG changes its PoA, when it sends a periodic RS, or when another mMAG requests the connection to the network. The entity that performs this triggering is the connection manager that is capable of choosing the best available connection and tries to connect to it through an RS message. This connection manager implements a periodic RS dispatch that maintains the connection always on. The Binding Cache Entry (BCE) has a timer that will expire if no RS message is received; if that timeout happens, the entrance relative to the mMAG will be deleted. There are several possible situations that may occur depending on the state of the BCEs and the network. The most relevant ones will be explained here:

- **A new mMAG tries to connect to the MAG:** In this case the BCE will not exist for this node neither in the MAG nor in the LMA.

  Therefore, when the mMAG sends a RS to the MAG (that will be its serving MAG),

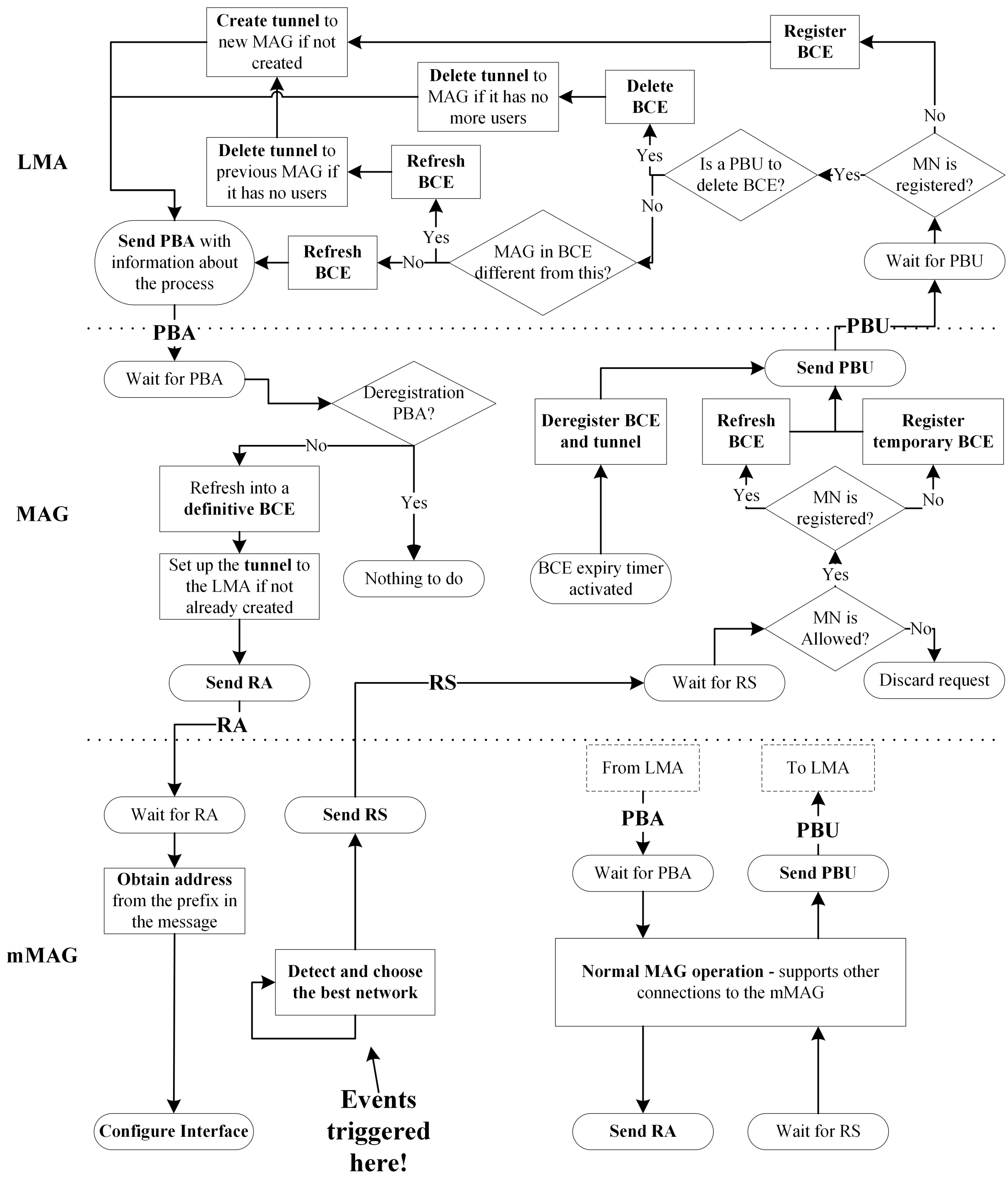


Figure 3.3: Representation of N-PMIPv6 operation

this will start verifying its access permissions. If they check out, and as the mMAG is not registered in the BCE yet, that registration will follow with a temporary BCE entry that will only become permanent when the LMA confirms the validation of the registration.

Upon the temporary registration is performed, the LMA is informed about the node request through a PBU message. This message will in its turn trigger the registration of the mMAG in the LMA's Binding Cache (BC), and the creation of a tunnel to the serving MAG if it was not already created (the tunnel would be previously created if any other device was connected to that MAG before).

Thereafter, the PBA message would confirm to the serving MAG that the BCE entry was successfully created in the LMA, and the MAG will follow with the transformation of the temporary BCE into a permanent one and finishing the creation of the bidirectional tunnel LMA - MAG.

Consequently, the serving MAG would follow with the transmission of the RA to the mMAG containing the intended prefix. With the prefix information and the interface MAC address, the mMAG will generate the IPv6 following with the configuration of the IP in its interface.

- **The mMAG performs a handover:** When the RS is transmitted to the new serving MAG, the situation of the BCEs is the following: the node was already registered in the BCE of the LMA with a different serving MAG (that can be a MAG or a mMAG); it is not registered in the new MAG's BCE.

  In this case, when the RS arrives to the new serving MAG, and if the node is allowed, the process in the MAG will be similar to the previous one and a new temporary BCE will be created.

  Upon the transmission of the PBU, the LMA sees that a BCE entry already exists but with a different serving MAG than the one that sent the PBU. In this case, the LMA recognizes that a handover has been performed and that the node is now accessing the network from a new network. Therefore, the previous serving MAG connection will be analysed in order to eliminate that previous tunnel if there are no more users that need it. If it does not exist yet, the tunnel to the new serving MAG will be created to allow the communication.

  When the PBA is transmitted, the MAG will, as in the previous case, configure the BCE entry as permanent, finish the tunnel creation and send a RA that allows the mMAG to configure its interface according to the provided prefix.

- **The mMAG is already connected to this serving MAG (periodic RS):** If this happens, then the mMAG is already registered both in LMA and MAG's BCE.

  Upon the reception of the periodic RS and the verification about the mMAG allowance, the serving MAG verifies that it already has the mentioned entry relative to this mMAG. First, it resets the timeout timers, then, it sends the PBU to the LMA which, in turn, also resets the timers.

Afterwards, the PBA message will be sent to confirm the correct operation, the tunnel and BCE in the MAG will remain the same and the RA to the mMAG will be sent with the same prefix which will make no effect if its IP was already configured; if that IP was not in the interface anymore it will be configured.

- **An interface of the mMAG disconnects:** When the interface disconnects and the BCE times out, the BCE is deleted and a PBU will be sent to the LMA informing that the mMAG is no longer connected. The LMA will then act accordingly, deleting the BCE and the tunnel to the MAG if it is not being used anymore. Upon the reception of the PBA, the MAG will recognize that the interface's BCE was erased.

3.2.2 Multihoming

The multihoming extension for PMIPv6 was developed under PMIPv6, and it is a dynamic architecture capable of taking full advantage of each access network in the range of the user terminal. It integrates context information and maintains a valid traffic distribution rule in real-time without impairing the access networks' performance.

For this purpose, the solution keeps its main operation in the LMA device where three main entities were implemented. As explained earlier in these document, these entities are the TM that manages the user terminals and its interfaces; the FM that manages the flow's relation with the terminals, the traffic distribution, the rule calculation and its application; the IM that manages all the information about the status of the access networks. Furthermore, there are two more entities, the NIS and the UIS placed in the MAG device and in the end user device, respectively.

Given the fact that PMIPv6 does not have support to bind the different interfaces to a certain user, the TM entity fills that blank. It uses a list that can be located in the LMA or in the MAGs to relate the interface MAC address and the terminal during the permission access process. Moreover, it maintains a User Cache Entry (UCE) in the LMA that contains information about the user, namely the terminal identifier, the number of connected interfaces and a set of information about each connected interface. It is worth noticing that the terminal identifier is the prefix allocated to its interfaces (which will be the same to every interface of the same user).

Regarding the traffic, this multihoming approach also inserts an entity that detects it, calculates the best way to distribute it, according to the conditions of the network, and applies the calculated distribution. This is the FM: it maintains a Flow Cache Entry (FCE) per end user terminal which contains data about the flows of that terminal. The FCE contains a vast amount of information and statistics, identifying the user to which that FCE is related, its number of flows, the percentage of traffic that is allocated to each interface, timers and a number of information and statistics about each flow. The calculation of the traffic rule division is performed in the way that it minimizes the average time that packets

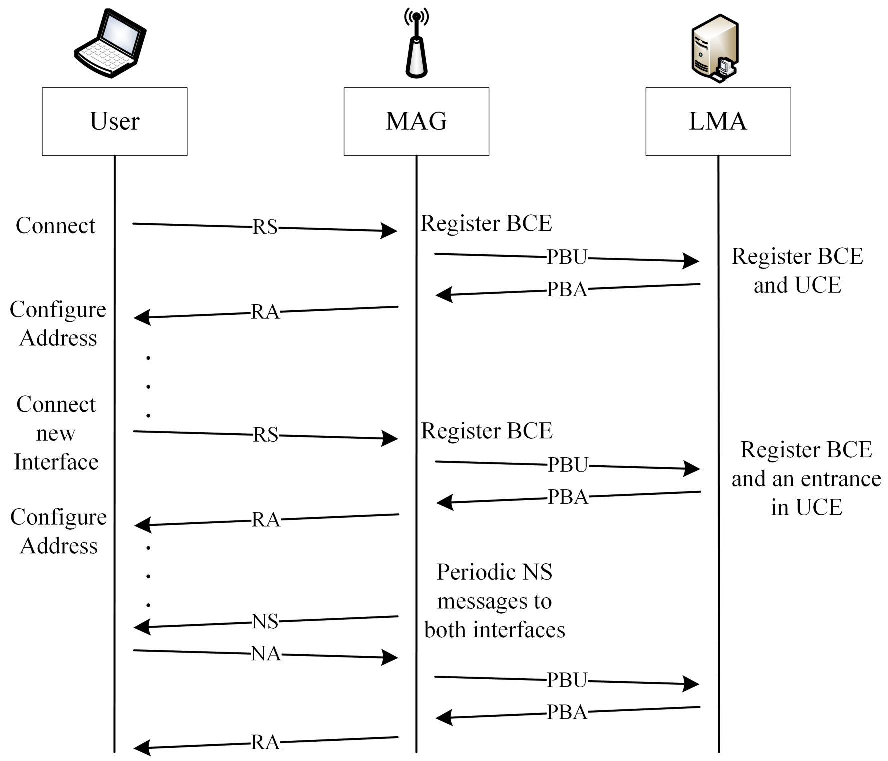


Figure 3.4: Representation of the multihoming operation related with the terminal and interfaces control

spend in the network, and when one packet is analysed, this rule is enforced and an IP replication is performed in the user side when the traffic starts.

In order to have all the real time information needed about the state of the networks, the IM, NIS and the UIS operate in a way that the information is taken to the LMA in a timely manner. In this way, whenever the FM needs to recalculate the rule, a request is performed to the NIS and UIS in order to obtain the necessary data which will be provided to the IM.

Within the scope of the integration between the N-PMIPv6 and the multihoming, the FM and the IM, as well as the NIS and UIS, are mostly autonomous and will simply operate in parallel with the interfaces and users management. In this way, this section will only analyse the TM entity together with the operation of the PMIPv6. The messages exchanged here are the same as in PMIPv6 and are represented in figure 3.4.

The operation method is shown in figure 3.5 and, as it is noticeable, the basis operation of PMIPv6 is the main content. Basically, the alterations are only noticeable in the LMA which is where the TM is located. The operation in the MAG is exactly the same as in PMIPv6 with the RS message to connect and the NS and Neighbour Advertisement (NA) messages to maintain the connection. In this way, the analysis will be mostly performed about the LMA.

The multihoming process, in what regards to the interfaces and users management, can be divided into several different cases according to the state of the caches and the state of the network itself. Consequently, the main situations will be analysed here:

- **User terminal has never been connected to this network and attempts the connection for the first time:** In this first case none of the caches have any entry regarding the interface or the user that is connecting.

  Firstly, when the device requests access to the network through the RS message, the MAG validates the interface and, as in the normal PMIPv6 operation, it creates a temporary BCE entry, and forwards the request to the LMA in the form of a PBU.

  Then, the LMA checks that the interface has no BCE registered, consequently creating one, and fulfilling the support for the exchanging of messages with the tunnel creation to the MAG that sent the PBU if it was not created already. After the interface has its own BCE, it is time to create a new UCE since the user was not registered with this interface, neither with another. With the UCE creation, an entry for the interface must exist, therefore an entry for the connecting interface is created in this user's UCE. Upon the interface and user registration, if the LMA has any traffic to this user, this is sent through the connecting interface.

  When this process in the LMA is finished, a PBA message that informs about the success of the process and about the prefix for the user is sent to the MAG. The BCE entry for that interface will be accounted as a permanent one, the tunnel creation is performed, and the received prefix will be sent to the User's interface so that it can be configured accordingly.

  After the registration, NS and NA messages will be exchanged periodically between the MAG and the user in order to validate the connection. Every time the user responds with a NA message, the expiry timers will be reset in the MAG, and a PBU will follow to the LMA so that it can also refresh its timers.

- **User terminal has one interface connected and attempts to connect another one:** In this case, and since each interface has a BCE, this cache entries will not exist for this interface because it is the first time that it connects. However, the user already has one interface connected, so its UCE is already created in the LMA.

  In this way, when the MAG receives the request from a new interface, if that interface is allowed, it creates a temporary BCE and forwards the request as a PBU to the LMA. The LMA will verify that the interface has no BCE entry, will create one and will also create a tunnel to the MAG if needed. Nevertheless, the UCE already exists and the LMA will, therefore just create a new interface entry in tha user's UCE. Also, if there is traffic, the rule of the traffic division will be refreshed, or created, so that the calculation can take into account the new interface.

  Afterwards, as in the previous case, the LMA wil send a PBA to the MAG which will, in its side, register the BCE as a permanent one, finish the creation of the bidirectional tunnel to the LMA and send a RA to the user terminal with its prefix.

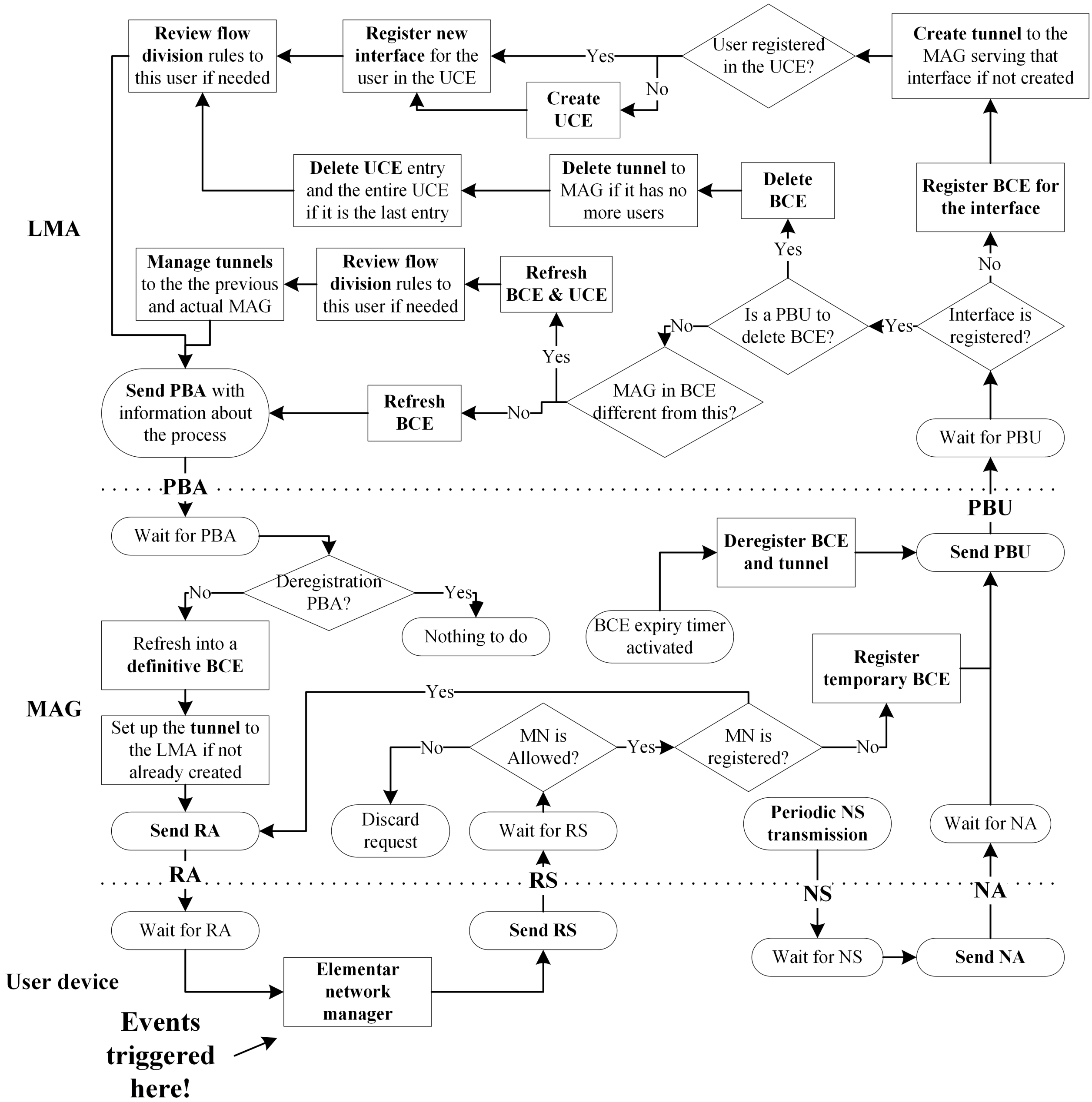


Figure 3.5: Representation of the multihoming operation related with the terminal and interfaces control

After the registration, NS and NA messages will be exchanged periodically in each connection, and every time the user responds with a NA message, the expiry timers will reset in the MAG, and a PBU will follow to the LMA so that it can also refresh its timers.

- **User terminal disconnects one interface:** When an interface is disconnected, the expiry timers will timeout and the MAG's BCE will be deleted. Upon that, a PBU will be sent to the LMA informing about the disconnection and the LMA will proceed with the de-registration process.

  LMA will start by verifying that the BCE exists and if the PBU is aimed at deleting the BCE. In this way, the LMA deletes the BCE entry, verifies if it needs to delete also the tunnel to the MAG (in the case that was the only interface connected to it, the tunnel is not needed anymore), and verifies what it needs to do with the UCE. If the UCE has more than one entry, it means that the user is still connected through another interface and the LMA just needs to erase the entry that corresponds to that interface. However, if the UCE has only one interface registered, then the LMA needs to delete not only that interface's UCE entry, but the entire UCE, since the user is not connected to the network anymore.

- **User interface performs a handover:** If this happens, then in the new MAG the BCE does not exist, but in the LMA both BCE and UCE exist for that interface. However, they exist with a different serving MAG associated.

  When the interface connects to the new MAG, this will perform the registration just like in the other cases. It initiates a temporary BCE and sends a PBU to the LMA.

  In the LMA the story is completely different. The LMA notices that the BCE entry exists for that interface, but that the PBU comes from a different MAG. Here the LMA notices that the interface has performed a handover and acts accordingly. It starts by refreshing the information present in the BCE and UCE about the interface and its serving MAG. Then, if there is traffic to that user, the rule of distribution is reviewed and finally, it deletes the previous tunnel if needed and creates a new one to this new MAG if it is not created already.

3.2.3 Combination of N-PMIPv6 and multihoming

The integration of N-PMIPv6 and multihoming has to take into account the differences between both solutions. Hence, some choices need to be made relating to which solution has a better performance in each case. In this way, the union of the two implementations needs to be the best suited to the restrictions and objectives of the present solution. In order to better understand the options in this field, the following features need to be taken into account:

- The high dynamics of the environment of a VANET implies that the solution needs to operate in the fastest way possible.

- The implementation of the solution in real OBUs and RSUs implies that the implementation should be as suited to them as possible.
- The usage of more than one network interface implies that their connection management is as optimized as possible.
- The implementation in a possible loaded network implies that the traffic scheduling should be as optimal as possible.
- The utilization implies that the vehicles should have always the best connection possible when in multihop or single hop.
- The utilization of this solution in a real scenario implies that the users inside the vehicle must not have the notion that any mobility happened. Their sessions must continue seamlessly.

Accordingly, taking into account the previous points, the N-PMIPv6 protocol was taken as a starting point to the combination of both. This alternative was taken due to the fact that N-PMIPv6 was already implemented in a VANET scenario and was optimized to work as a vehicular mobility solution, supporting several technologies including WAVE. Also, the support of mMAGs operation was already built into the N-PMIPv6. In the other way, the multihoming features are the ones being integrated, and not the main mobility protocol. In this way, the multihoming entities were integrated into the N-PMIPv6 operation.

Maintaining the main base of N-PMIPv6, the main concerns that relate to the dynamics of VANETs, interaction with WAVE interfaces and network mobility are accounted for, since the previous work was related to that subject. In the other side, the integration of the multihoming features will cover the several interfaces management and the division of traffic according to the state of the connections.

In figure 3.6 is visible the initial integration of both N-PMIPv6 and multihoming. Note that this representation does not have into account the information and traffic related features of multihoming as those features operate in parallel with the main operation of mobility and users management. Due to the fact that the base point was the N-PMIPv6, and the alterations that better cope with VANETs particularities were desired, the messages exchanged in the present solution are the same as in N-PMIPv6 which are shown in the figure 3.1.

As explained regarding N-PMIPv6, the mMAG is a mobile router that has the capabilities to move around and connect to different PoAs managing its own mobility. Due to the operation of N-PMIPv6, the mMAG can also connect to another mMAG in multihop. This multihop feature is performed just as it was in N-PMIPv6, the connecting mMAG always sees the upstrem nodes as a network and acts as a MAG downstream so that other mMAGs can connect to it.

Regarding to multihoming, the management of the users and its interfaces is performed in the TM entity that operates in the LMA along with N-PMIPv6. TM maintains a UCE for each user where the user prefix, the number of interfaces connected and relevant informations about each interface are stored. Also, the remaining entities of the multihoming

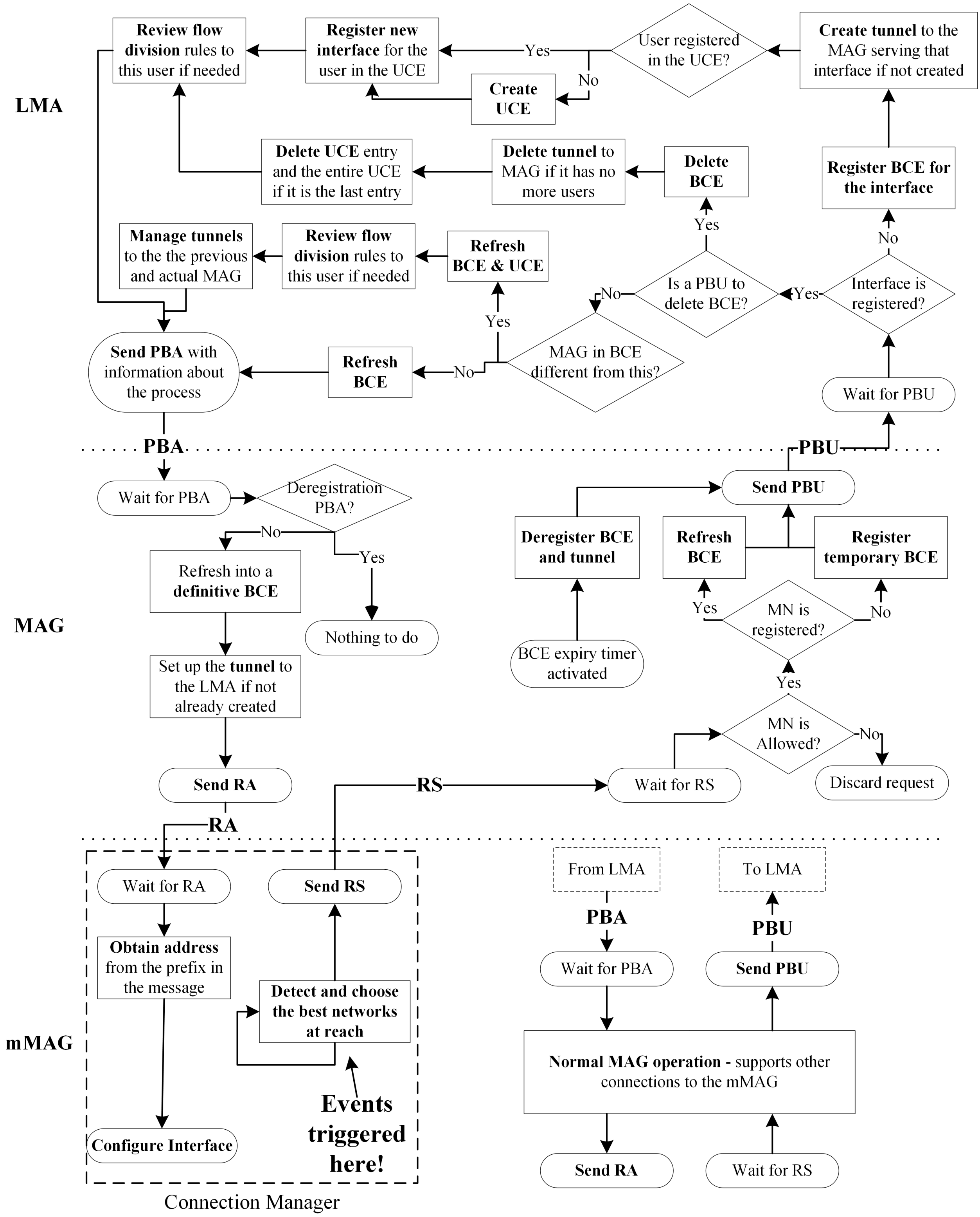


Figure 3.6: Representation of the operation of the initial integration of N-PMIPv6 with multihoming related with the terminal and interfaces control

extension for PMIPv6 are integrated with the solution. The FM will allow this solution to manage the flows for each user and distribute the traffic in an optimal way so that the average time that the packets spend in the network is minimized. In the other side, the information related entities (IM, NIS and UIS) are also integrated in a first approach of the solution guaranteeing that the FM has all the information about the network as it needs.

The operation of this implementation can comprise several situations. Depending on the state of the binding cache and the user caches, one mMAG's interface that sends one request can be treated in different ways. Some of the crucial ones are the following:

- **The interface of a mMAG that was not connected to the network tries to connect to one MAG:** In this first case this mMAG has no registration of any BCE to its interfaces neither of an UCE in the LMA.

  If the interface is allowed through the security restrictions, the normal operation of registration of a temporary BCE will be followed in the MAG by the transmission of a PBU to the LMA. The LMA will register the BCE to this interface, the UCE to this user and the UCE entry for the interface. Among these registrations, a tunnel will be created to the MAG and the FM will be informed that an alteration has occurred. Afterwards, the PBA will be sent to the MAG which will register the BCE as a permanent one, finish the tunnel creation and inform the mMAG of its prefix through a RA message.

- **mMAG has one interface connected and tries to connect another one:** The same as in the multihoming solution, the BCEs for that interface do not exist, but the user already has an UCE in which this interface is not registered.

  In this case, the MAG creates the temporary BCE and forwards that interface request to the LMA in the form of a PBU. The LMA also creates the interface's BCE and introduces an entry in that user's UCE with the interface information. It also manages the tunnel to that MAG (the serving MAG) and informs the FM about the changes. Then a PBA message is sent downwards so that the MAG can register the definitive BCE and inform the mMAG's interface of its prefix through a RA message.

- **One mMAG tries to connect to another mMAG through one of its interfaces:** The operation of multihop is based on the fact that the mMAG is nothing more than an enhanced MAG. It operates as a MAG when another mMAG tries to connect to it and the tunnel created to the LMA goes through the tunnel already created to connect the previous hop. Basically, the PBUs and PBAs are sent through that tunnel to the LMA and back in a way that the operation is done just like in a common MAG. Hence, this operation is performed in the same way as in the previous cases.

- **The interface that is already connected sends a periodic RS:** A periodic RS means that the interface was already registered in the BCEs and in the UCE. Like in the N-PMIPv6 operation, the request passes through the MAG refreshing the BCE and timers, goes to the LMA where it also refreshes the BCE and the timers. In this case there is no need to refresh the UCE, since it does not bring new information. Afterwards, the LMA acknowledges the request to the downstream devices.

- **mMAG interface performs a handover:** When an interface performs a handover, the operation is almost the same as in N-PMIPv6. The request goes through the new MAG that creates a temporary BCE and forwards the request to the LMA in the form of a PBU. In its turn, the LMA verifies that the BCE exists, but with a different serving MAG. Hence, it will refresh the BCE and UCE entries with the new information, it will manage the tunnels to the new and old serving MAG (delete the old one if not used and create the new one if needed), and finally it will inform the FM about the change and acknowledge the request.

  Upon receiving the PBA, the MAG registers the permanent BCE, finishes the creation of the tunnel and informs the mMAG about its prefix with an RA message.

- **An interface of the mMAG disconnects:** In the case a BCE of an interface expires in a MAG or mMAG, a PBU will be transmited to the LMA informing that the mMAG's interface is not connected to that MAG anymore. In that case, the LMA will eliminate the interface BCE, its entrance in the UCE or the entire UCE if no more interfaces of that mMAG are connected.

The fact that the mMAG is capable of roaming and connecting to another MAGs and mMAGs is explained with the existence of a connection manager entity (which is represented in the figure 3.6). This entity is responsible to initiate the connection process and maintain the connection. With multihoming, a simple connection manager is not enough and a multihoming one needs to be developed. This solution will be described in further detail in section 3.4

3.3 One interface multihoming

WAVE is a broadcast based technology with no session establishment like in Wi-Fi which implies that the usage of one interface can be much more flexible. In this case, one interface can send the same message to more than one neighbour in their WAVE interface (broadcast), or send two different messages to two different WAVE neighbours without having to exchange any control message or perform any handshake process. In this way, as explained in figure 3.7, one OBU can act as if it had 'n' WAVE interfaces where 'n' is the number of connections to WAVE neighbours it aims to have. Moreover, this can be any type of connections like V2V in multihop to another OBU or V2I when connecting to an RSU. One WAVE interface can communicate with them all without losing performance.

Figure 3.7 shows one case in which one WAVE interface is used in several links and the connection is performed seamlessly. Following this thought, it is possible to use this as an advantage to apply in multihoming. If one vehicle (mMAG) can connect to several MAGs

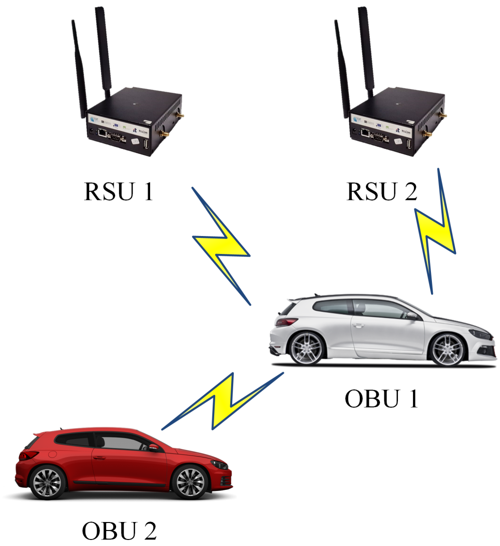


Figure 3.7: One OBU communication with several other devices with just one WAVE interface

---

and/or mMAGs, and the network recognizes this as a multihoming connection, this can bring advantages in the load distribution of the network.

Using this interface to perform several connections to the network will allow the traffic distribution algorithm to distribute the traffic that has that user as destination through more paths and, therefore balancing the load on the network.

In this sense, and since the interface management in the LMA is based on the MAC of the mMAG's interface, there is a need to extend the identification so that the several paths to the user are distinguished. As explained in the section 3.2.3, the LMA identifies each interface of the mMAG with one BCE entry. In the base implementation of the BCE, everytime the LMA receives a PBU from an existent mMAG and from a different serving MAG, this is seen as a handover which is not what is aimed here. Hence, this BCE entry needs to be extended in order to support the identification of the several paths as different entries in the BCE.

In an effort to identify the differences between those paths, one main distinction was made: each connection will have a different combination of the interface MAC address and the serving MAG IP (IP of the MAG or mMAG to which the present mMAG is connected to). The analysis of this feature can be divided into two parts:

- The address of the interface can be the same, if the same WAVE interface is used to more than one connection, but, in that case, the serving MAG IP will be different since the mMAG will not request two connections to the same PoA. Two RS messages to the same PoA are needed to maintain the connection.

- The IP of the serving MAG can be the same to two different connections, but, in that case, the MACs of the interfaces connecting to it will be different because, again, one

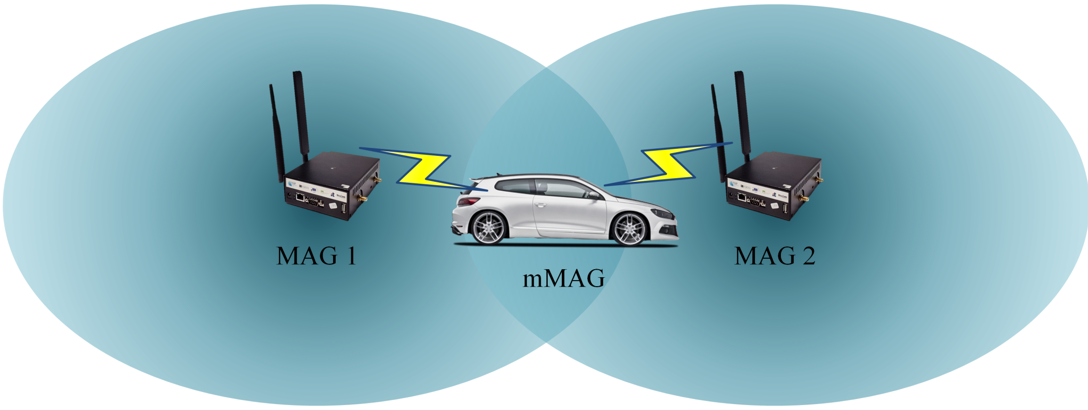


Figure 3.8: The usual situation, mMAG goes through an area in which it can communicate to both MAGs before losing the range of the previous one (range overlapping)

interface will not connect two times to the same MAG. If the serving MAG identifies two RSs from the same interface, they will serve as a refreshment of the connection.

In this way, the identification of the mMAG's interface in the LMA will be made through its serving MAG IP and the interface MAC address. Note that the interface of a mMAG is identified by its MAC address because, if the IP addresses are replicated in two interfaces, this will be the only distinct address.

This approach brings a difficulty in the handover detection. As the operation of the LMA starts by verifying if the interface has a BCE entry, with this new approach the BCE will not be recognized as belonging to the same interface in the case of a handover. If the mMAG's interface connects to a new MAG, the PBU that reaches the LMA will have information of a different combination of the interface and serving MAG IP's, therefore it does not recognize the previously registered BCE with a different serving MAG. Hence, the LMA will create a new BCE entry to this new path. Nevertheless, the real handover situation in this case never really happens because the handover would imply that the communication would cease in one path and start going through the other in one given moment. Even if the range of two MAGs would not overlap, but would still border each other, and the mMAG would go through that exact spot, either the reach to the first MAG would be lost before it connects to the next one, or it would be connected to the two at the same time. In the most usual situations, the ranges of two PoAs are overlapped in some space which allows the mMAG to communicate through both paths in multihoming during some time. Figure 3.8 can illustrate about the usual situation when one mMAG is about to leave the range of one MAG and reach the range of a different one. As we can see, when in the overlapped region, the mMAG will be in multihoming communicating through both paths at the same time.

In this way, with an appropriate BCE expiry time, the connection would be refreshed and the LMA would be informed about the disconnection of the mMAG from the previous path in a useful time. Besides, when the RSSI of a certain connection starts going low, the traffic distribution rule will stop using that path if there are the means to accommodate all the traffic through better paths. In order to accommodate this improvement, when the connection manager verifies that the RSSI of a certain connection goes below a certain threshold, it sends a non periodic RS which caries the information about the RSSI and informs the MAG about the state of this connection. In its side, the MAG will evaluate that value and besides the normal PBU, it will send an information message to the LMA that will be interpreted as a sign to recalculate the traffic division rule in the way that it will try to cease the use of that path given the low RSSI. The exchange of these messages is shown in the figure 3.9.

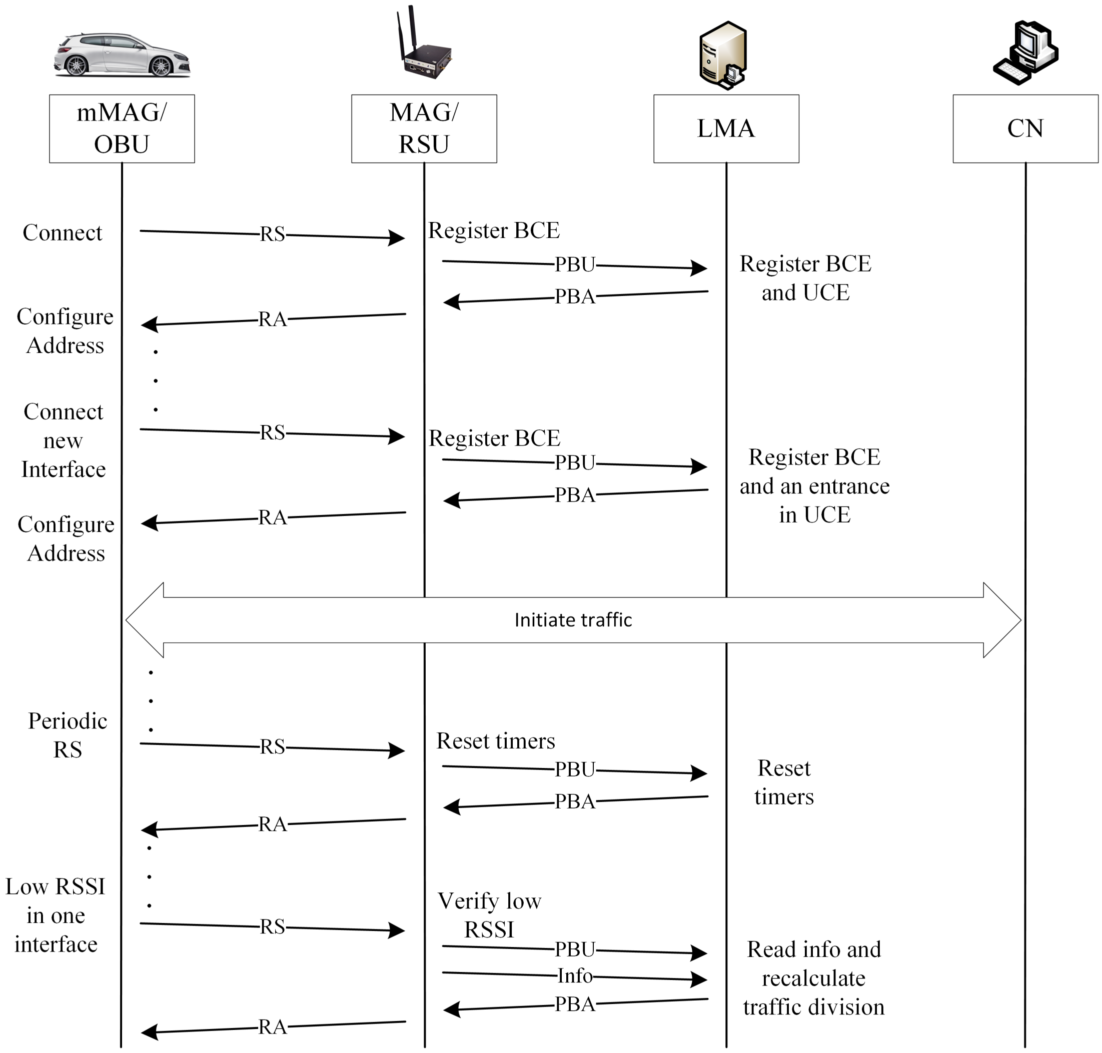


Figure 3.9: The connection manager senses that the quality of the connection is going low, it sends an extra RS and the MAG informs the LMA

With this functionality, the LMA operation will be different. As the figure 3.10 depicts, two blocks (in blue) were changed in the LMA operation, and also the ones that correspond to the handover treatment were eliminated. With these changes, the first verification is about the combination of the interface MAC address and the serving MAG IP registration, in opposition to the previous verification about only the MAC address of the interface. The other changed block was the registration of the BCE entry, appending the address of the serving MAG to its key.

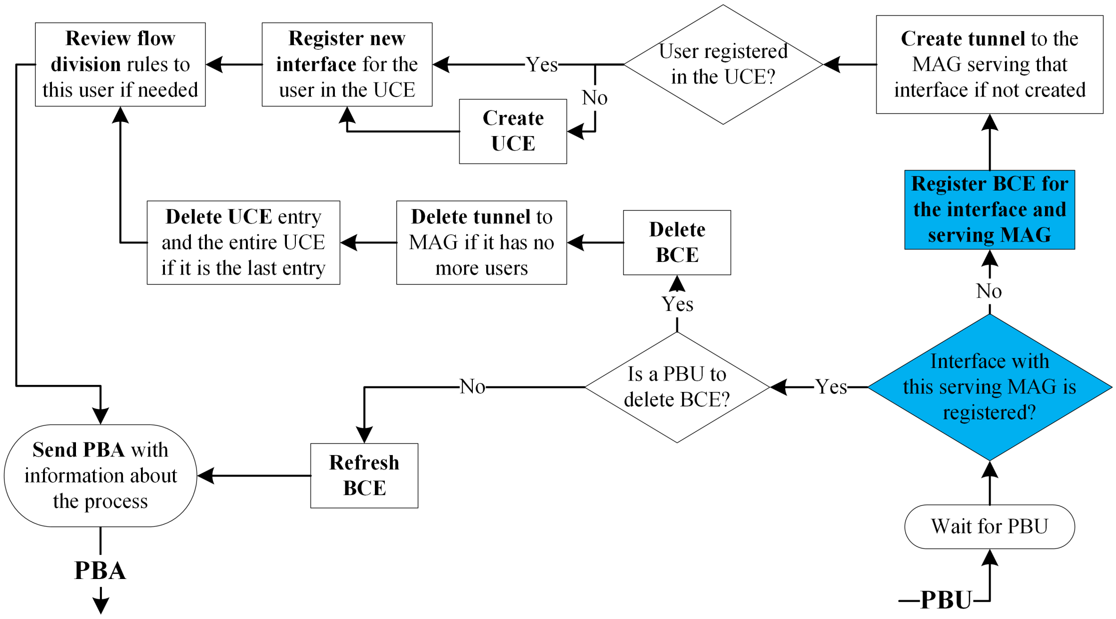


Figure 3.10: Operation method of the LMA with the multihoming support and assuming the connection to two PoA with one WAVE interface

3.4 Multihoming connection manager

In order to support the mobility of a mMAG, an entity that requests connection, manages the periodic messages and configures the interfaces needed. In this way, a simple connection manager that targets only mobility was developed in another dissertation and is used here as a starting point to develop an enhanced one for multihoming support. This base mobility connection manager is able to scan the networks available in two technologies, WAVE and Wi-Fi, sending then a RS to the WAVE PoA with better RSSI if it exists or else to the Wi-Fi PoA with better RSSI. Also, it does receive the RA that acknowledges the RS and configures the respective interface with the received prefix and the Extended Unique Identifier 64-bit (EUI-64) [71] suffix that corresponds to the respective interface. Moreover, this connection manager sends the periodic messages needed to maintain one connection.

However, a more advanced connection manager is needed in order to fulfil the needs of multihoming. The objective here is to support the connection of the mMAG to another mMAGs or/and to MAGs through the use of WAVE and Wi-Fi technologies that are available in the OBUs and RSUs.

According to the explanation of this solution in section 3.2.3, the messages needed to connect and maintain the connection from the mMAG connecting side are just the transmission of RS messages and the reception of RA messages. In this way, a RS is sent to the PoA in order to firstly establish the connection, and then periodic RSs are sent so that the connection is not lost. Also, an extra RS is sent when the RSSI level becomes low. Accordingly, one RA is received for each RS sent.

Therefore, there are several aspects that need to be taken into account in multihoming that were not supported by the previous connection manager:

- **Connection to more than one technology simultaneously:** In order to use the multihoming technology, the mMAG must be able to have more than one connection. Therefore, taking advantage of the fact that the OBUs support more than one technology, two of the network interfaces are used, namely the WAVE and the Wi-Fi. WAVE is the dedicated VANET technology that has several adjustments to its environment, and Wi-Fi is used as a complement to the first one. With the different characteristics of the technologies, different arrangements are performed to each one. These arrangements include different periodicities of scanning the available networks, different connection criteria, and different usage criteria, and will be further explained in this section and also in the next chapter.

- **More than one connection in WAVE:** With the adjustment performed to the operation of the solution, namely the usage of more than one connection to the same WAVE interface, there is a need to support also that improvement in the mMAG side. In this way, the connection manager has to be able to choose, request and maintain several connections with the WAVE interface.

- **Configuration of more than one interface:** If the mMAG sends RSs to more than one PoA, it will also receive several RAs in return. This implies that it has to be capable to receive them, and configure the respective interface accordingly, independently of the number and interface of the requests it receives. This configuration is performed every time the mMAG receives one RA. The RA contains a prefix allocated by the LMA that will be used to the autoconfiguration of the interface's IPv6 through the concatenation with the EUI-64 [71] which is based on the interface MAC address.

- **Dynamic uplink routes:** In the initial mobility connection manager, the uplink default route was a simple and easy parameter to implement, the route would just be through the path through which the mMAG is connected. However, with multihoming there are as many possibilities as the number of active connections, and therefore a criterion should be taken. As this was not the focus of the work, the most plausible solution was taken: route the uplink traffic through the WAVE path which has the best RSSI. However, if there are no WAVE connections available the traffic is routed through the available Wi-Fi connection. Once this default route is established, in order to avoid rapid switching between several paths with close RSSI values, an hysteresis level is assumed in the way that the route will only change if the new best network has a RSSI value higher in a certain configurable number.

- **Connection criteria:** With several possibilities of connections, with multihoming the mMAG will not just connect to the best network at reach; it will connect to several of the best networks at reach. In this way, a norm must be taken in order to choose the best networks available for a possible connection. Regarding the WAVE interface, a minimum threshold is established where the only networks to which the mMAG will connect are the ones with a RSSI higher than that threshold value. In the case of Wi-Fi networks, a minimum threshold will not be considered because this interface will only be considered as a backup interface where non urgent traffic will be routed through. Therefore, in Wi-Fi, the network with the best RSSI will be chosen if the velocity of the vehicle is not too high or if there are no more connections available.

  Also, there is another difference in the criteria between WAVE and Wi-Fi usage in the periodicity of the scan for best networks. While in WAVE the time taken to perform that scan is very low, and the connection process is also very fast, then the scanning periodicity can be very low allowing a fast adaptation to the changes in the surrounding networks. In the other side, the Wi-Fi technology is much slower in the scan and in the connection procedure. The simple scan procedure takes approximately one to two seconds, therefore obliging the scan periodicity to be in the seconds scale. Moreover, while scanning, the interface needs to go through the several frequencies which does not allow the communication in that time. Consequently, in order to save resources in Wi-Fi and improve the quality of the connection, if the quality of the link of the actual Wi-Fi connection is a good one, the scan will not be performed and the actual connection will be maintained.

- **Maintain several connections:** In the base version of the connection manager the periodic messages were just to the one link to which the mMAG was connected. But in this case periodic messages have to be sent to every PoAs to which the mMAG is connected to, implying a more careful managing of those messages to be performed.

In this way, the operation of the multihoming connection manager is divided into three main parts: Wi-Fi operation, WAVE operation and RAs Reception. This will be explained in the following sections.

3.4.1 Wi-Fi operation

Regarding the operation in Wi-Fi, figure 3.11, the scans are periodically performed with a configurable period. This periodicity is defined in the way that the changes in the surrounding environment are noticeable in a timely manner, and also in the way that the scan can finish its operation before the time to start the next period.

The first step to be performed once it is time to perform another scan is the verification of the velocity. This allows the program to know if the car is, or not, going too fast for

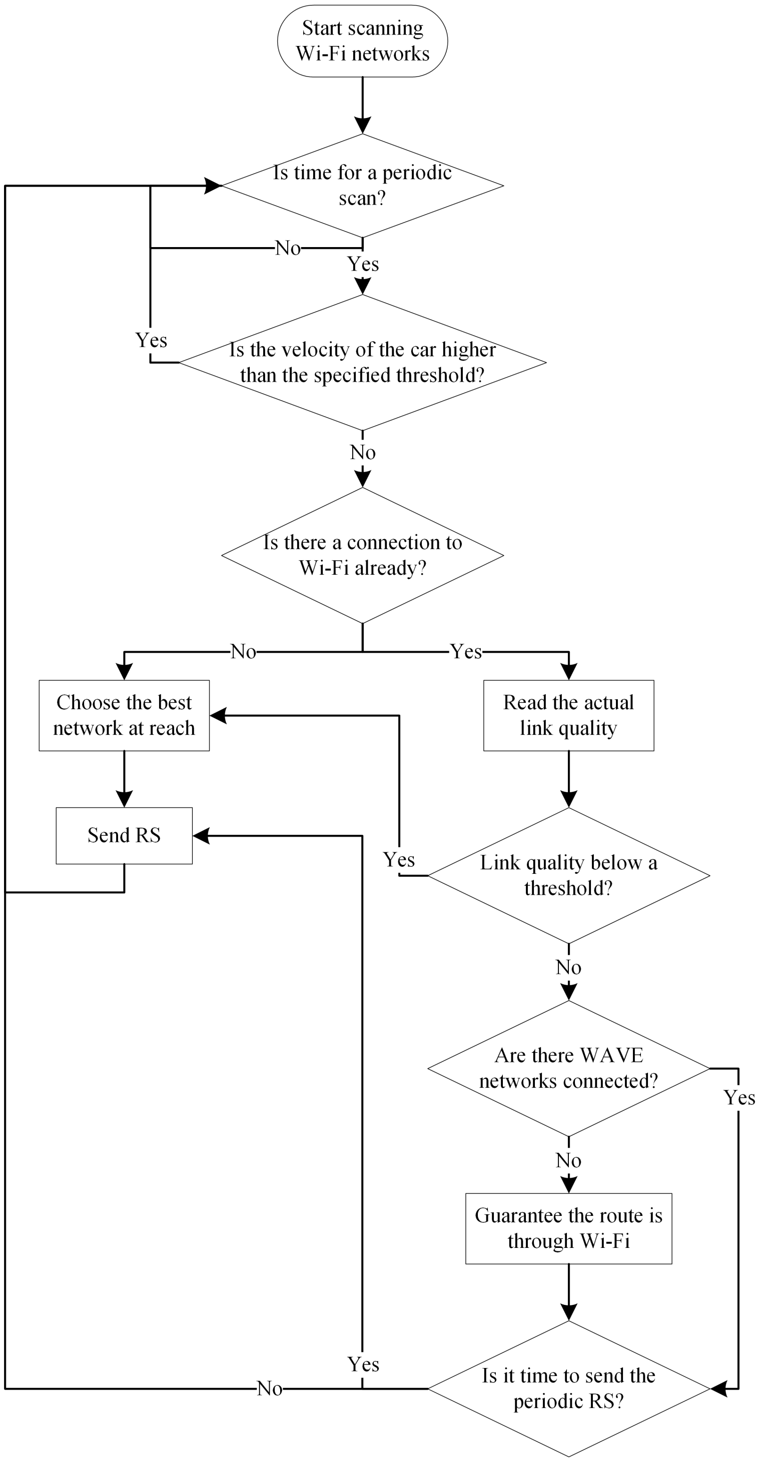


Figure 3.11: Operation method used in the connection manager to connect to Wi-Fi networks

the use of Wi-Fi to be profitable. The Wi-Fi connections are discarded for high velocity because this technology has a relatively low range and the connection is costly in terms of time due to its association process. Otherwise, if the vehicle is going at low speed, there are two possibilities in what regards the state of the Wi-Fi connection, either there is none or one connection established. In the first case, the connection manager will simply check what are the best connections available and try to connect to the best with an RS message. In the second case, in order to avoid the constant scan of the medium and minimize the resources utilization, the state of the actual connection is verified. If this verification detects a good connection, then there is no need to check for a better network and only the route and periodic messages need to be verified. Otherwise, if the verification notices a bad link quality, a scan is performed to attempt to get a better network assuming a certain hysteresis level.

With respect to the uplink default route verification, the route is only allocated to the Wi-Fi network if there are no WAVE connections available.

Finally, the verification about the periodic messages is performed. In this way, the time from the last RS sent to this PoA will be checked, and another one will be sent if the periodicity time has passed so that the MAG/mMAG knows that this mMAG is still connected.

3.4.2 WAVE operation

In WAVE operation, which is shown in the figure 3.12, the scan is much more frequent than in Wi-Fi. This is because the WAVE technology is much faster than Wi-Fi, since it was developed specially thinking about its use in the VANET dynamic environment. Contrarily to Wi-Fi it is broadcast based, has no session establishment and its range is much higher. In this way, and because the scanning of the available networks is much faster, the scans are more frequent.

Whenever a scan needs to be performed, each network has to be analysed and not just the best one as in Wi-Fi. This is due to the fact that we are using the WAVE interface to connect to several WAVE PoA. With this feature, every reachable MAG is a candidate to be chosen as one PoA.

In the analysis of a network, one distinction can be made from the beginning: the mMAG can be disconnected to that PoA or it can be connected to it. Starting from the first case, if it is not one of the connections of the mMAG, the connection manager will evaluate if the RSSI level is higher than the minimum defined level to connect. Hence, if the RSSI and the expected connection time are high enough, the connection manager will send a RS asking for the connection to that network. In the other side, if the mMAG is already connected to that network, it will firstly evaluate if that is the network that corresponds to the uplink route. If so, the connection manager updates the value of its RSSI so that it can in the end be compared to the best network RSSI in order to check if the change of this uplink default route is needed.

Afterwards, a verification of the RSSI level is performed. If this level is lower than the level defined to disconnect, an extra RS message is sent to the MAG with the information

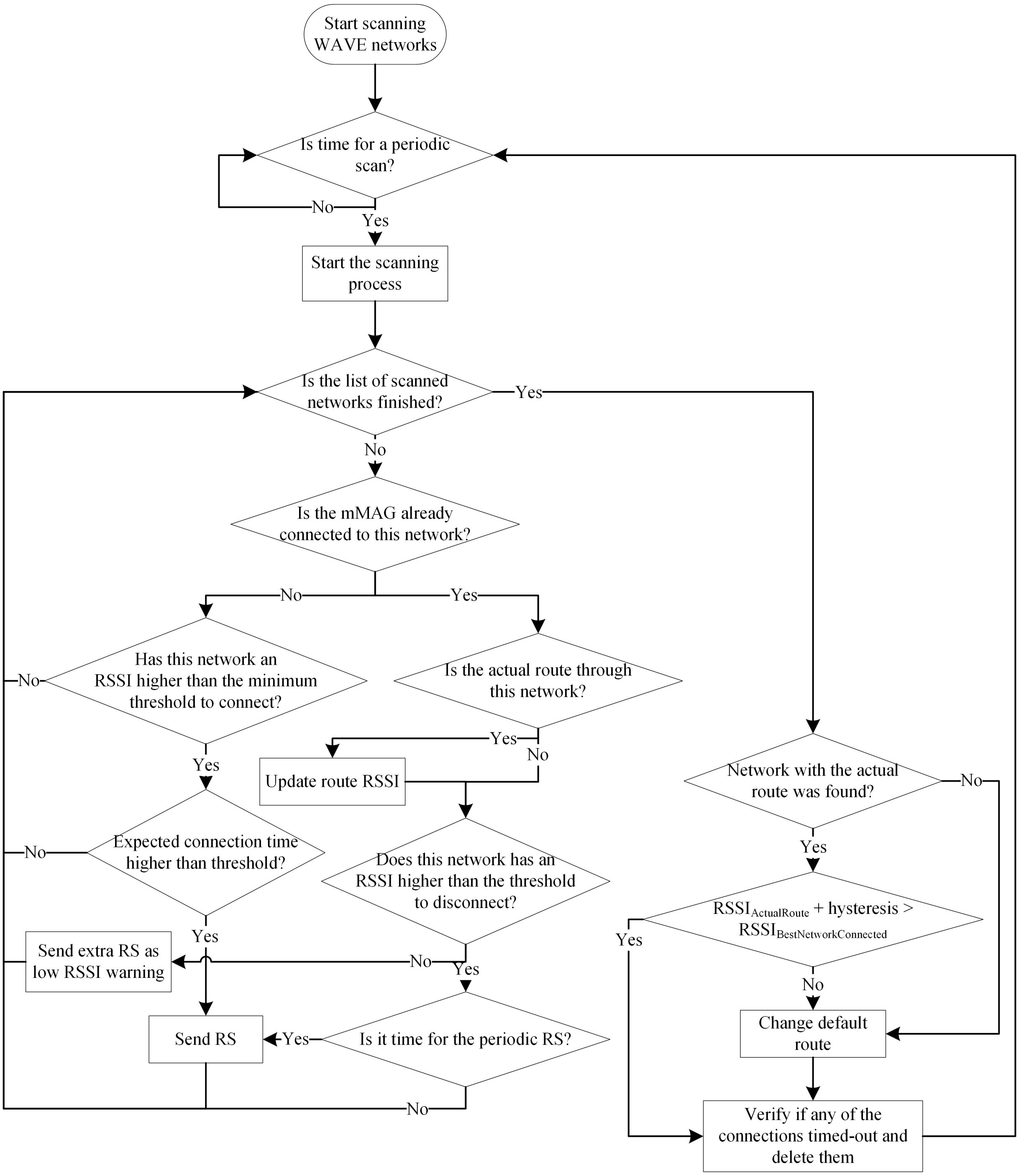


Figure 3.12: Operation method used in the connection manager to connect to WAVE networks

about the RSSI, so that the MAG can warn the LMA that the mMAG's interface may be disconnecting. As a measure to prevent the fast change of this decision, an hysteresis is implemented so that the connect threshold is higher than the disconnect one.

If the connection manager decided to maintain the network, then it will be verified if the time to send the periodic RS has come, and if so, it will be sent.

When all the reachable networks are analysed, it is time to recheck the default route. The route will be changed in two situations: if the network that corresponds to the actual route was not found, or if the RSSI of the best network is higher than the RSSI of the actual route added with a certain programmable value of hysteresis. The mentioned hysteresis will allow the default route to be maintained if there are two networks with similar levels of RSSI instead of a possible case of rapid switching between both.

Lastly, the verification of the connected networks needs to be performed. This verification will check for how long those networks did not receive RAs, and it will delete the entries of those which have a time higher than the expiry time.

3.4.3 RAs Reception

In order to complement the two other operations that send RSs to connect to a network or to refresh the connection, another entity is needed that is capable of receiving the response messages (RAs). This entity receives these messages, configures the respective interface and also takes part in the definition of the default uplink route. Its operation is shown in the figure 3.13.

The RAs process starts with the reception of one packet. It first checks if that received packet is a RA destined to the mMAG in question and, if this premisses do not check, the packet is discarded.

In the other side, if the first verifications are surpassed, the connection manager builds an IPv6 address based on the prefix received in the RA packet and the EUI-64 based on the MAC of the interface. This IP is meant to be allocated to the interface, and if it is not already allocated, the interface through which the RA was received will be configured.

Depending on the technology of the interface through which the packet was received, different operations will follow. In the case of Wi-Fi, only operations regarding the default route will be performed. In this case, if there are no WAVE connections the route should be through Wi-Fi. If the route does not exist through Wi-Fi or the network corresponding to the existing route is not the one in study, the default uplink route should be updated to this one.

On the other side, if the interface through which the RA was received was the WAVE one, the first operation is to check if that network was registered on the connected ones or if it is a new connection. In the case it is a new connection, then the network is registered and the default uplink route is defined to that PoA if there was no route to WAVE networks. Finally, the expiry timer of the entry corresponding to this network is reset either if the network was already registered or not.

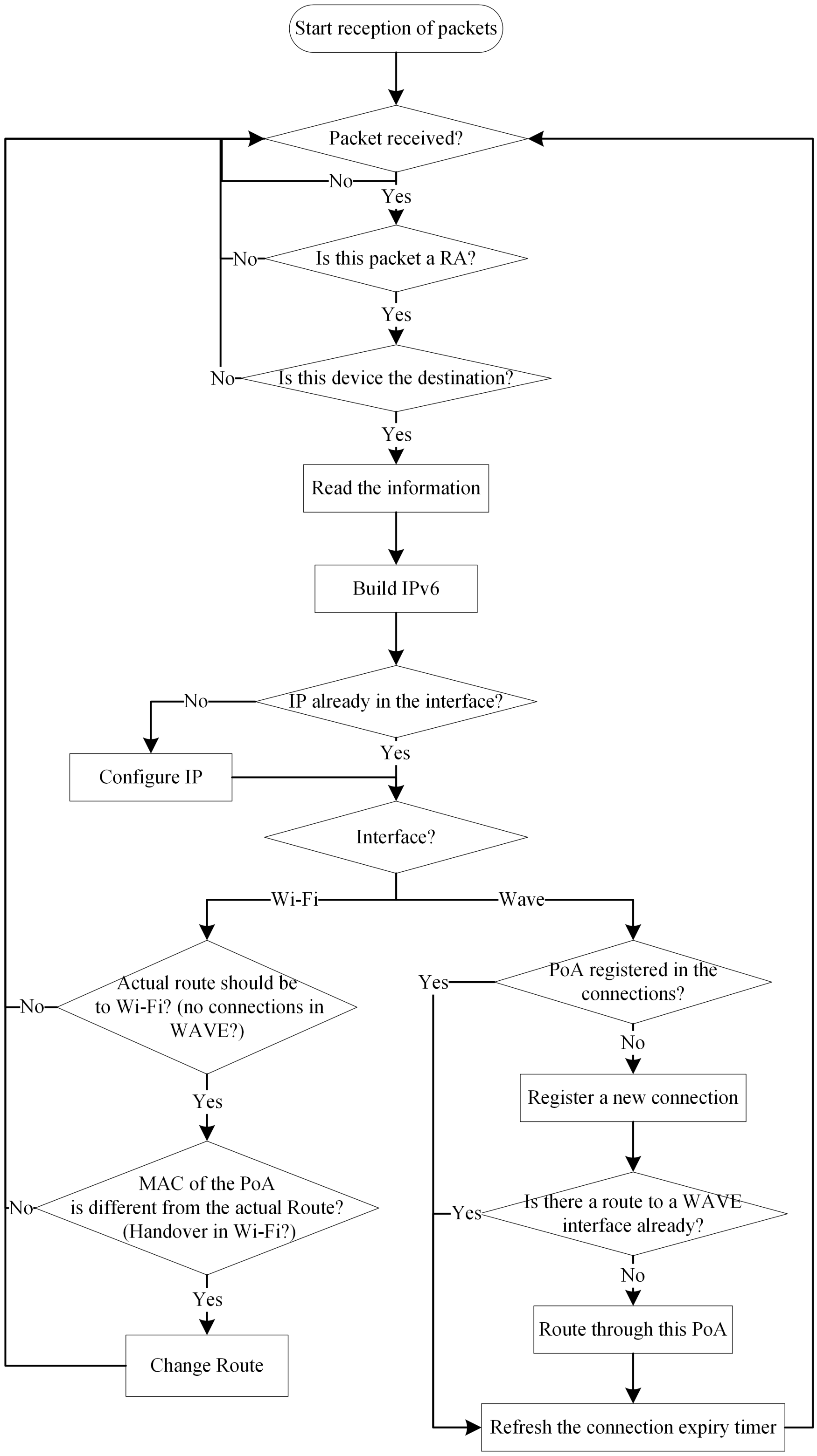


Figure 3.13: Operation method used in the connection manager to receive RAs and configure the interface accordingly

3.5 Mobility and multihoming rule adaptation

With the migration of the multihoming functionalities to a vehicular scenario the velocity becomes one of the main issues. In the less dynamic environment in which the multihoming was developed, the concerns with time consumption were not as important as in VANETs, and therefore, the multihoming approach needs to be refined. One of the most important and most time consumption feature is the determination of the traffic distribution rule.

Also, another important feature to take into account in this point is the usage of three technologies with different restrictions. WAVE is the main technology to use when compared to Wi-Fi since they have a different time consumption and range, and when compared to cellular due to the cost and structured architecture of cellular. In this way, the most time sensitive traffic should be relayed through WAVE if possible; if not, it should go through cellular due to the low quality of Wi-Fi in dynamic environments. This was not an issue in the previous implementation of multihoming since the WAVE technology was not used and the environment was not that dynamic. Therefore, the most time sensitive traffic and the more suited paths should be identified, and the traffic should be relayed accordingly. This feature can be implemented along with the rule calculation and application. This section will mainly consider the multihoming rule with both WAVE and Wi-Fi. The cellular integration, performed in the parallel dissertation, will be described in the next section.

Relating to the rule that was implemented in the PMIPv6 multihoming extension that was taken as base for this implementation, it is part of the FM entity and is specified in [7] and [72]. It minimizes the time that the packets spend in the network, therefore the end-to-end delay, using the information obtained by the IM entity about the PoAs statistics and information like the capacity, the mean packet size and the mean packets per second that flows through them. For this calculation, it also gets some information about the connection between each PoA and the end-user terminal, namely its available bandwidth, achieved throughput and packet loss. At each time the rule is calculated, a request is performed from the LMA to the MAG so that the necessary information is provided. In its side, the MAG can easily provide the information about the characteristics of the PoA since they are constantly monitored, but in the other side the characteristics about its connection to the end-user terminal have to be measured using an extension of Wbest [73], which is based on packet pair and packet train techniques. Only after this process, and after the information is received in the LMA, a genetic algorithm is used to calculate the optimal percentage of the traffic that should go through each path in order to minimize the average time that the packets spend in the network. Upon the calculation, the division is performed in a packet basis without distinction about the types of traffic or the technology of the connection.

Therefore, for the implementation in VANETs several changes need to be performed. These changes are related with the creation of a simple distributed and fast process that can distinguish the traffic and distinguish through what kind of interface this traffic is being sent through. This traffic can be internet traffic, sensors data and information, videos to the users, software updates for the network and much more. Therefore, the classification and different treatment of this traffic is important.

In this way, the base operation of multihoming was improved in order to support a distributed rule calculation that considers also the classification of the traffic in levels of priority, the classification of the paths through its technology, number of hops, possible early disconnection and the group of flows through the type of traffic. An overview of this operation is shown in figure 3.14.

The operation starts just as in the original one with a verification to check if the time for the periodic calculation was reached or if there were relevant changes in the network, like the connection or disconnection of one network. If any of these points are checked, the rule determination starts. This operation will be described in the next sections.

3.5.1 Flows identification and ordering

In order to better understand the classification and identification of the traffic, one must first understand the granularity of the traffic analysis. This granularity is shown in figure 3.15 and identifies the packets, which can be aggregated in flows, that are mainly sequences of packets from a source to a destination which, in their turn, are grouped into types that represent the type and priority of the traffic (e.g. real time/ non-real time). Lastly, every mMAG has its traffic which is analysed individually.

The identification of the type of each flow is performed based on the port used by its traffic, and when the flow is inserted into the FCE, it is inserted in a position that corresponds to the priority of the port it is being transmitted through. In this way, the flows of the priority groups (types) are already in sequence which allows the grouping process to be easier. Therefore, when treating the groups and flows, the task will be more simple since they will be ordered by priority, and those with higher priority (first ones in the FCE) will be the first to be accounted for. The insertion of new flows is shown in the figure 3.16 where the number of each group corresponds to its priority, and if one flow is to be inserted, it is inserted in the end of that group.

In what regards to the grouping, this is done because, if the flows have characteristics that are alike, then there is a possibility that they will be correlated and, if we can lower the delay difference between their packets by sending the group through one path, that chance should be taken (when one sends the packets through two different paths, it is likely that they will have different delays and reach the destination with a different timing). With this approach the out-of-order packets within the flows will be reduced, leading to a lighter packet processing. Also, it is possible to guarantee that, if they fit in the traffic allocated to one high quality path, the most prioritized group will be sent through that path, and the same will happen with the next groups. This feature allows all the traffic with similar characteristics (that may as an example correspond to one type of application) and with high priority to be sent through the best path.

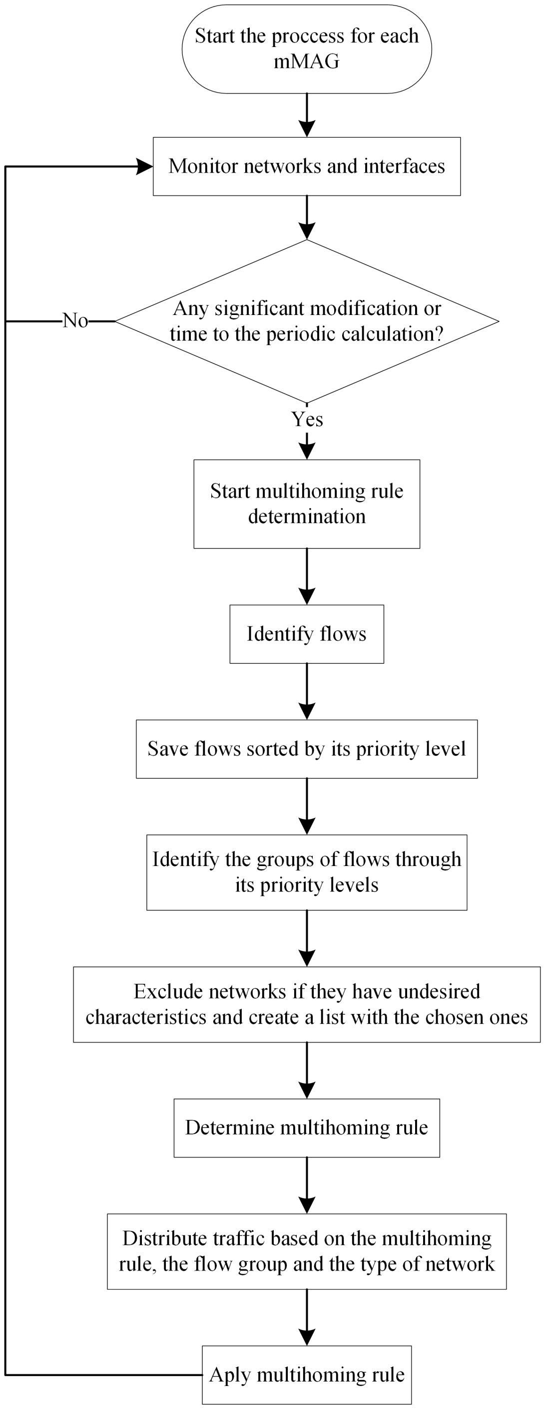


Figure 3.14: General operation of the new traffic distribution rule

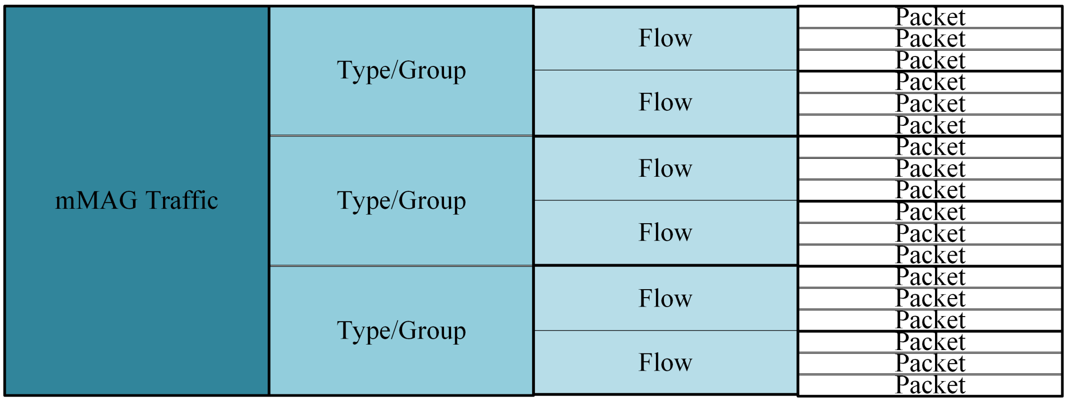


Figure 3.15: Granularity of the classifications and grouping of the traffic

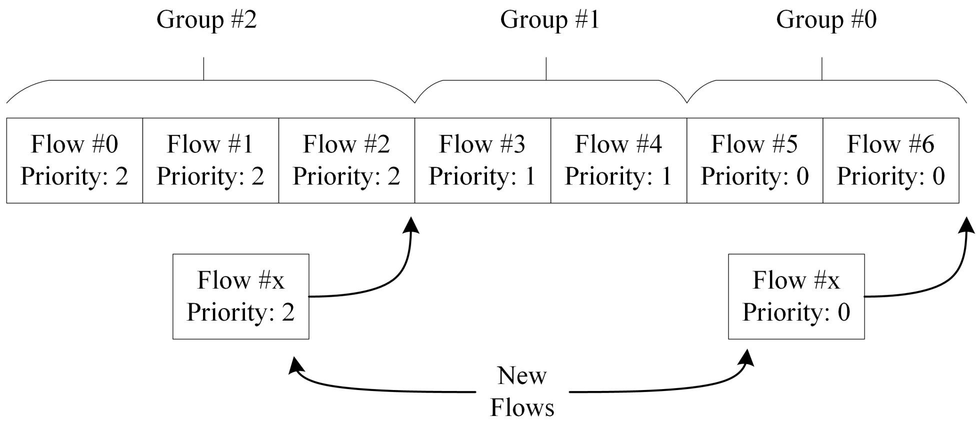


Figure 3.16: Insertion of a new flow in the FCE

3.5.2 Information retrieval and networks classification

Contrarily to the assumed multihoming implementation, in this case some of the informations that the IM obtains from the MAG and mMAG to calculate the rule are different. In an effort to lower the time spent in the rule calculation, the Wbest analysis of the connection is eliminated, and some different data is sent to the LMA.

The figure 3.17 shows the messages exchanged by the various entities so that the information needed to properly calculate the rule reaches the LMA. Firstly, the RSSI information is sent through the periodic RS message in some of its reserved bytes, allowing the storage of this information in the MAG. Besides, the technology through which the RS is received by the MAG/mMAG is sent in the PBU and stored in the LMA.

When the LMA starts the calculation of the traffic distribution rule, it sends a request to the MAG so that it can provide the information needed to that computation. In its side, the MAG sends back its statistics (capacity, the mean packet size and the mean packets per second) and the information of the mMAG (RSSI) that will be used in the rule calculation

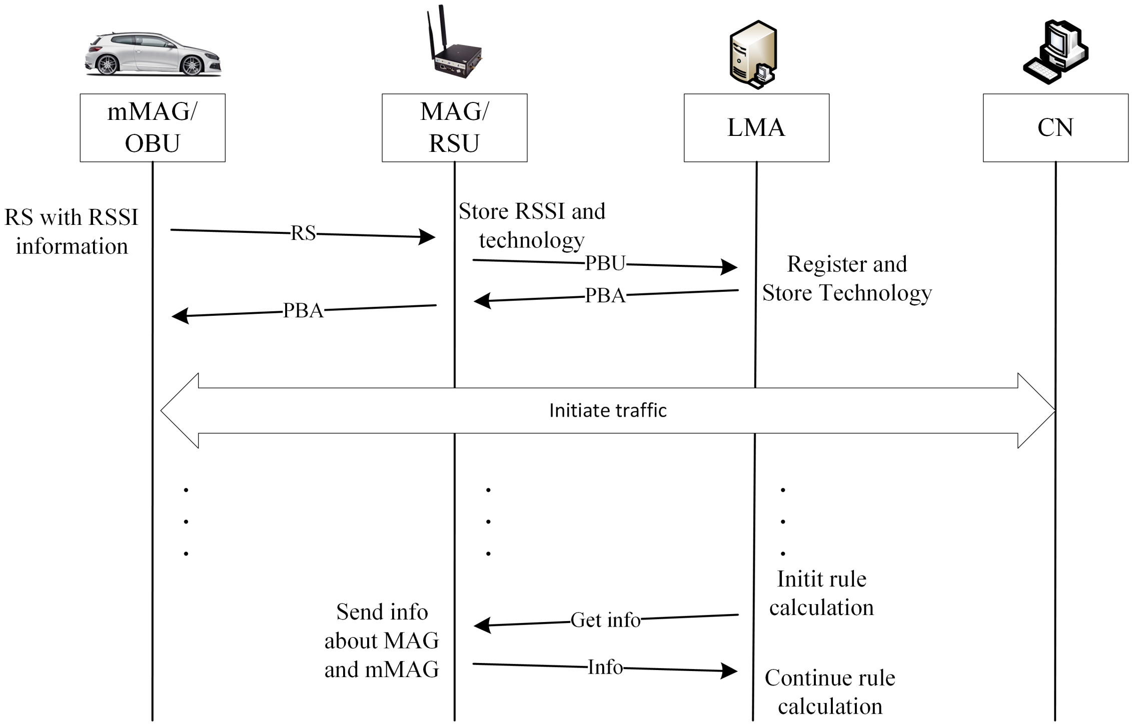


Figure 3.17: Messages exchanged that allow the information to reach the LMA

---

process. The Wbest analysis of the connection to the mMAG is not performed in an effort to lower the time of the process, and the information related to it, used in the LMA, will be a theoretical value.

The networks classification in its side is done in a distributed manner. This classification is represented in figure 3.18 in which several criteria act as an input. These criteria are listed and explained below:

- **Velocity of the vehicle:** Velocity is an important factor to take into account, since with vehicles it can vary a lot. Taking into account the differences between the used technologies, the WAVE connections should take place allways if the expected connection time of the vehicle is high enough, while for Wi-Fi, it will only connect if the velocity is lower than a certain configurable value. This measure is applied in the connection manager and is taken because it is known that, besides the Wi-Fi range is not large, the time it takes to connect is also not that good and therefore when, in high velocities, the useful data transmitted would be very low or even null.

- **RSSI of the connection:** The first stage of this measurement is performed in the connection manager. Besides having a minimum RSSI to connect to a WAVE PoA, the connection manager also informs the LMA if a PoA's RSSI goes below a certain level (lower than the one selected to connect). This will implement a hysteresis that allows the mMAG to connect to a certain PoA only if it provides a good link,

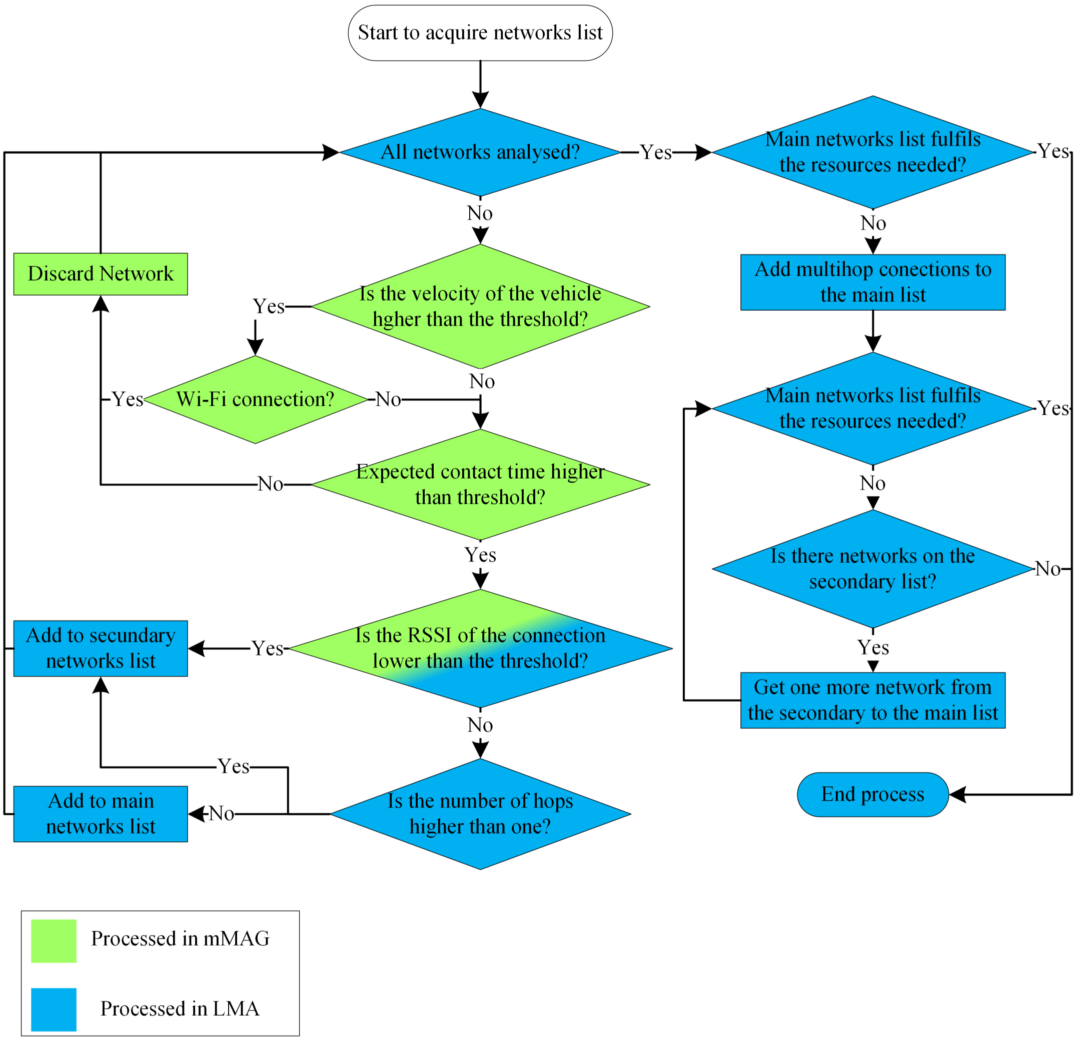


Figure 3.18: Operation flow of the distributed process of the constitution of the main networks list

otherwise, it stops the connection if it reaches a lower RSSI level. Also, if the RSSI for one specific connection is low, the LMA will try to avoid to send traffic through that path.

- **Expected contact time:** Another factor that should be taken into account is the expected time in which the mMAG will be in contact with that MAG. If this time is too low, the connection would not be profitable, so it should not take place.

- **Technology:** This time in the LMA side, the paths that go through WAVE technology are favoured in a way that the most important groups will be sent through them, while the least important traffic or the traffic that will not fit in the WAVE paths will be sent through Wi-Fi.

- **Number of hops:** Although the functionality that recognizes the number of hops in the LMA is not implemented yet, the distribution rule is prepared to take the number of hops into account favouring the direct connections with the most prioritized traffic.

Taking into account this criteria, a list will be created in the LMA with the most relevant paths, and another list will be maintained with the secondary paths that will be used only if the main ones are not capable to fulfil the traffic needs of the mMAG. This primary list is the one that is going to be analysed in the genetic algorithm, to define the percentage of the traffic that should go through each path, minimizing the average time that the packets spend in the network. If the capacities of the paths selected are not enough to fulfil the needs of the mMAG in terms of traffic throughput, then before calling the algorithm, paths from the secondary list will be added to the primary list so that the network can cope with the traffic needs of the user.

3.5.3 Determination of the traffic division and distribution of groups and flows

Using the information about the MAG retrieved earlier, the LMA calculates the inputs to the genetic algorithm. It also estimates the achieved throughput (that was in the previous version obtained through the Wbest analysis) taking into account the theoretical capacity of the MAG and the information about traffic that is flowing through it. The data that is used also takes into account the traffic that the multihoming process is inflicting on the system and does the calculations without it, so that the obtained values can observe the paths without the influence of the traffic to which we are calculating the rule to.

The genetic algorithm utilized is described in [72] and was used in order to allow the extraction of optimal values independently of the number of interfaces. This method is based on biological systems which always evolves to better fit and adjust to a certain problem, and its main advantage is its robustness. It is mainly based in three variables:

- Population: Represents a set of solutions which in this case are several different divisions.
- Chromosome: Represents one of the solutions in the population.
- Fitness function: Is the function that tests each chromosome and evaluates its quality for the scenario under analysis.

For each generation of the genetic algorithm, except for the first one in which the values are random, the genetic algorithm performs the reproduction, crossover and mutation to obtain the elements of the next generation. These processes perform, respectively, the selection of the chromosomes depending on their fitness, its combination and its possible alteration.

To stop the creation of new generations and new solutions, the following condition is taken into account: "If the best fitness of each generation presents, sequentially and during a certain number of generations, a difference between them below a certain threshold, the optimization process is terminated". In the limit, if this condition is not confirmed, the process will stop after a limit of generations. In the end, the chromosome with best fitness is taken.

Table 3.1: Notation

Symbol	**Definition**
N = $\{n_1, n_2, ..., n_{\|N\|}\}$	Set of point-of-attachment
λ_n	Mean inter-arrival rate at n ϵ N
μ'_n	Mean service rate of each n ϵ N
ρ_n	Occupancy ratio of each n ϵ N
σ_n	Fraction of MH traffic through n ϵ N
β_n^2	Mean service time variance of each n ϵ N
r^{MH}	Input rate of MH traffic

With the specification of the notation present in the table 3.1, the fitness function is represented in the equation 3.1 where N represents the set of PoAs available to perform multihoming and the following applies:
$\rho_n = \frac{\lambda_n}{\mu'_n}$
$\lambda_n = r^{MH} * \sigma_n$
$\mu'_n - \lambda_n < 0$
$\sum_{n \in N} \sigma_n = 1$

$$Minimize \sum_{n \in N} \frac{\frac{\lambda_n^2 \beta_n^2 + \rho_n^2}{2(1-\rho_n)} + \rho_n}{\lambda_n} * \sigma_n \tag{3.1}$$

The expression presented in this fitness function represents the average time that the packets spend in the system according to an M/G/1 model that approximates the real environment.

After using the obtained data to determine the traffic distribution rule, the groups will be divided through the paths chosen. Starting by the most prioritized group, the analysis depicted in the figure 3.19 is performed. First, if it is not the less prioritized group, a verification is performed to see if the group was going all through one network, if the actual traffic still fits the available space in the actual network and if this network is one of the main ones chosen. If these conditions are fulfilled, the group will continue to go through that network in order to minimize the changes. If it does not fit, then the best network will be analysed and if it does fit in that one, the group is allocated to that network and the next group is analysed; but if it does not, the division of the flows of the same group is minimized as well as the division of each flow. Note that, if the traffic belongs to the less prioritized group, then it will be distributed in a packet basis according to the rule obtained through the genetic algorithm and the percentage allocated specifically to other flows/groups. The percentages used in this packet division are obtained from the

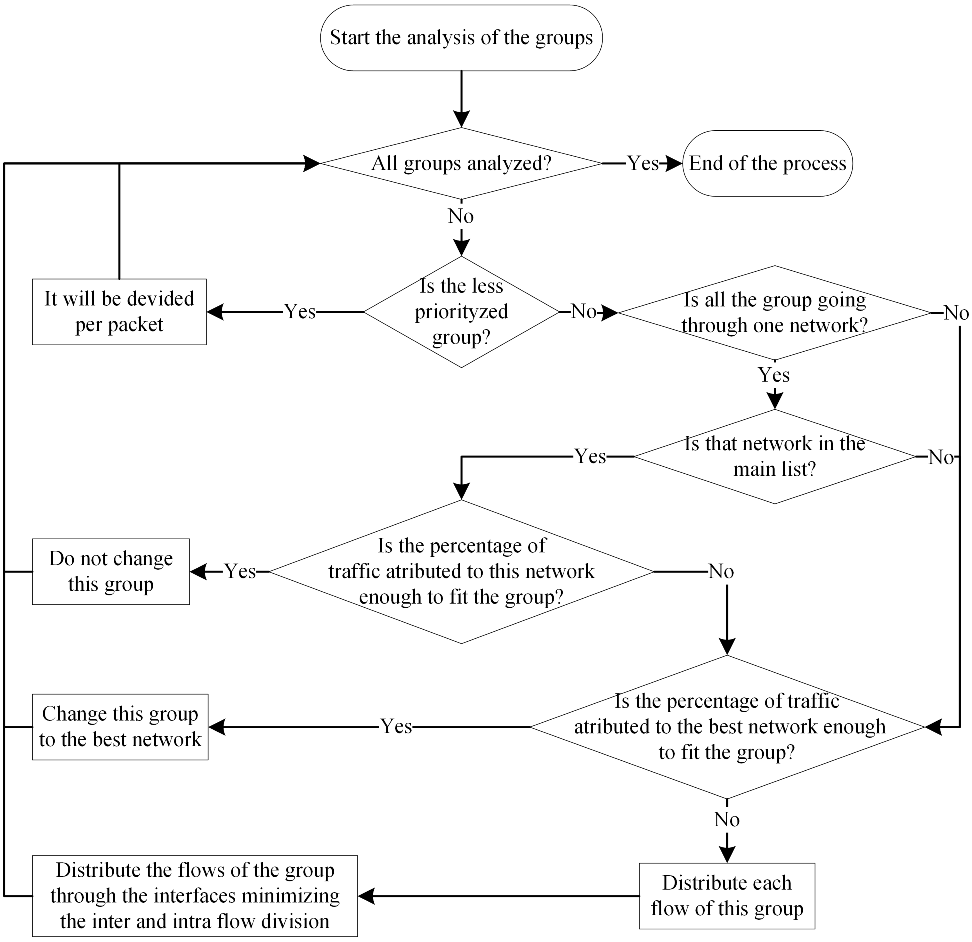


Figure 3.19: Operation flow of the distribution of the traffic through the interfaces

subtraction of the percentages allocated by the genetic algorithm and the already allocated percentages in this distribution.

Regarding the last block of the group division, "Distribute the flows through the interfaces minimizing the inter and intra flow division", it is further explained in the figure 3.20. In this block, the LMA tries to divide the flows of one group through the available interfaces. It starts by verifying flow-by-flow if they fit entirely in the available 'space' in the best WAVE network, trying to allocate the most flows possible in the same network. This best network is the one that has the more available percentage of the total traffic after the previous allocations. If there is one flow that does not fit entirely in that path neither the newly calculated path with more available 'space' (the path with more available space can change because flows are being assigned to it), but its percentage surpasses the allocated percentage for the best path in a small value, it is still allocated to that network.

In the other side, if the flow under analysis is too big to fit the best network plus a small value, the Wi-Fi networks are analysed and used to fit the entire flow if they have enough capacity available. Last, if the entire flow does not fit in any of the networks

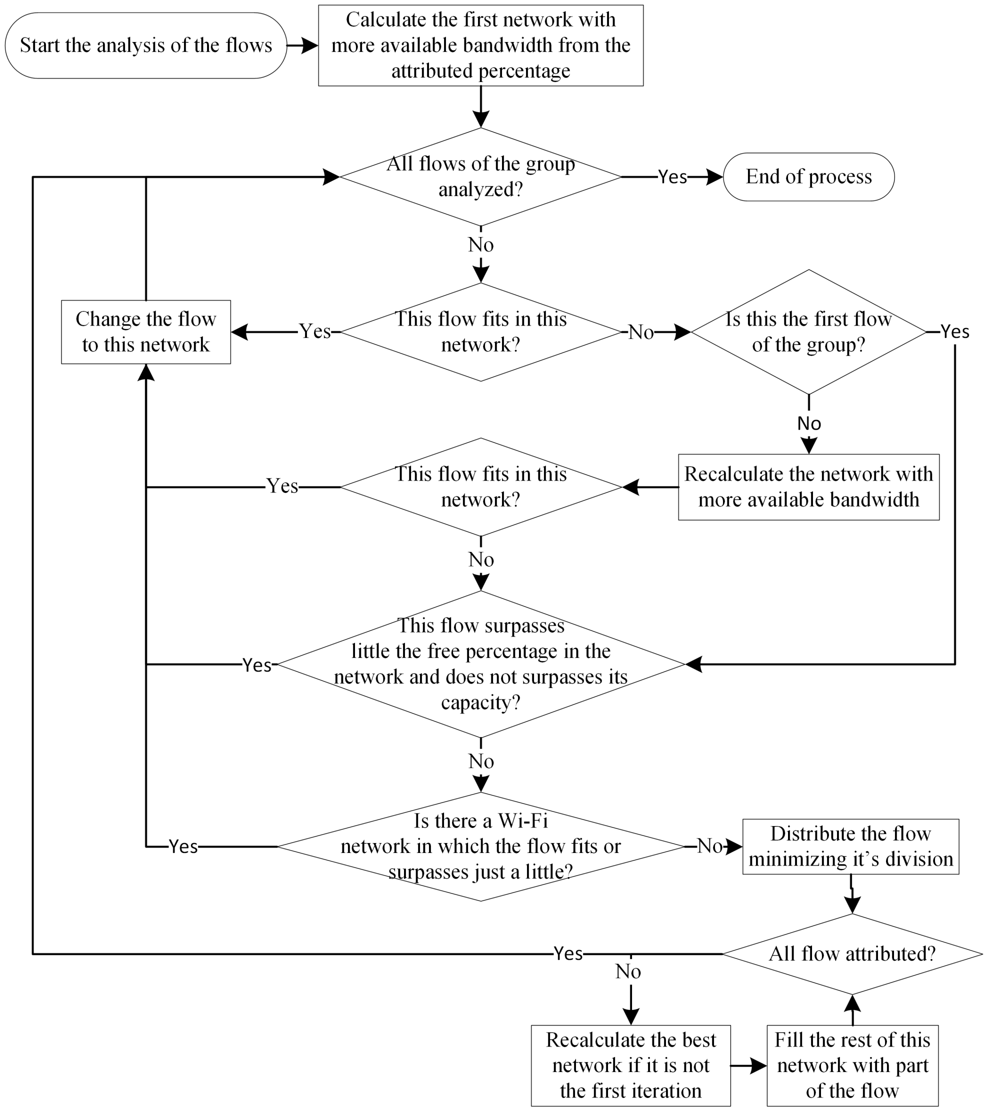


Figure 3.20: Operation flow of the distribution of the flows of one group through the interfaces

considering the allocated optimal percentage of traffic, it is distributed filling the available spaces of each of the networks. Therefore, this operation tries to accommodate the most flows possible from one group in the same network. In this way, the network to which the flows are being allocated is the same until there is one flow that does not fit there and, if this happens, the best network is recalculated and the process repeats. This leads to less division of the group's flows and optimizes the time of this operation through the minimization of the best network calculation.

Finally, the allocated path will be identified for each packet that goes through the LMA. This packet can encounter four hypothesis:

- The group to which the packet corresponds has a path allocated: The packet will be forwarded through that path.
- It does not have a path for its group but has a path allocated to the flow: The packet is forwarded through the path indicated to the flow.
- It does not have a path for the group neither for the flow, but the flow is divided in an optimal way. If the flow does not fit in any of the paths according to the optimal rule, it will be divided in an attempt to minimize the number of paths it uses.
- It belongs to the less prioritized group: if it belongs to the less prioritized group, the packet distribution rule will be applied according to the occupied percentages of the previously allocated ones to each path.

3.6 Integration with complementary dissertation

It was previously mentioned that another dissertation was running in parallel with this one. This other dissertation focused also on some of the features of the mobility and multihoming protocol, and both implementations were merged together into an improved version of this solution. To summarize, the main features of the final version are listed bellow:

- Support of full network mobility for the vehicles and for the users inside them.
- Utilization of multihoming to take advantage of all available resources in the vehicular network environment.
- Utilization in a vehicular network with Wi-Fi, WAVE and cellular as access network technologies.
- Integration with a Multihoming Connection Manager that manages the connections and configurations of the OBUs.
- Dynamic adaptation of the multihoming rule that distributes the multihoming traffic, in order to better fit the characteristics of VANETs and its traffic.
- Classification of the traffic according to its priority and posterior distribution of the flows through the available connections of a user, taking into account its characteristics.
- Support of multi-hop communications.
- Provision of internet via an IPv4 network to the users inside the vehicles either in single-hop or multi-hop connections.
- Simultaneous connection to more than one access point with the same or different interfaces of an OBU.

3.6.1 Integration of the cellular networks with the distribution rule

In order to integrate the work developed around the cellular connection in the complementary dissertation with the dynamic traffic distribution rule, the operation of classification of the networks is altered relatively to the one presented in the figure 3.18, which resulted in the operation specified in figure 3.21.

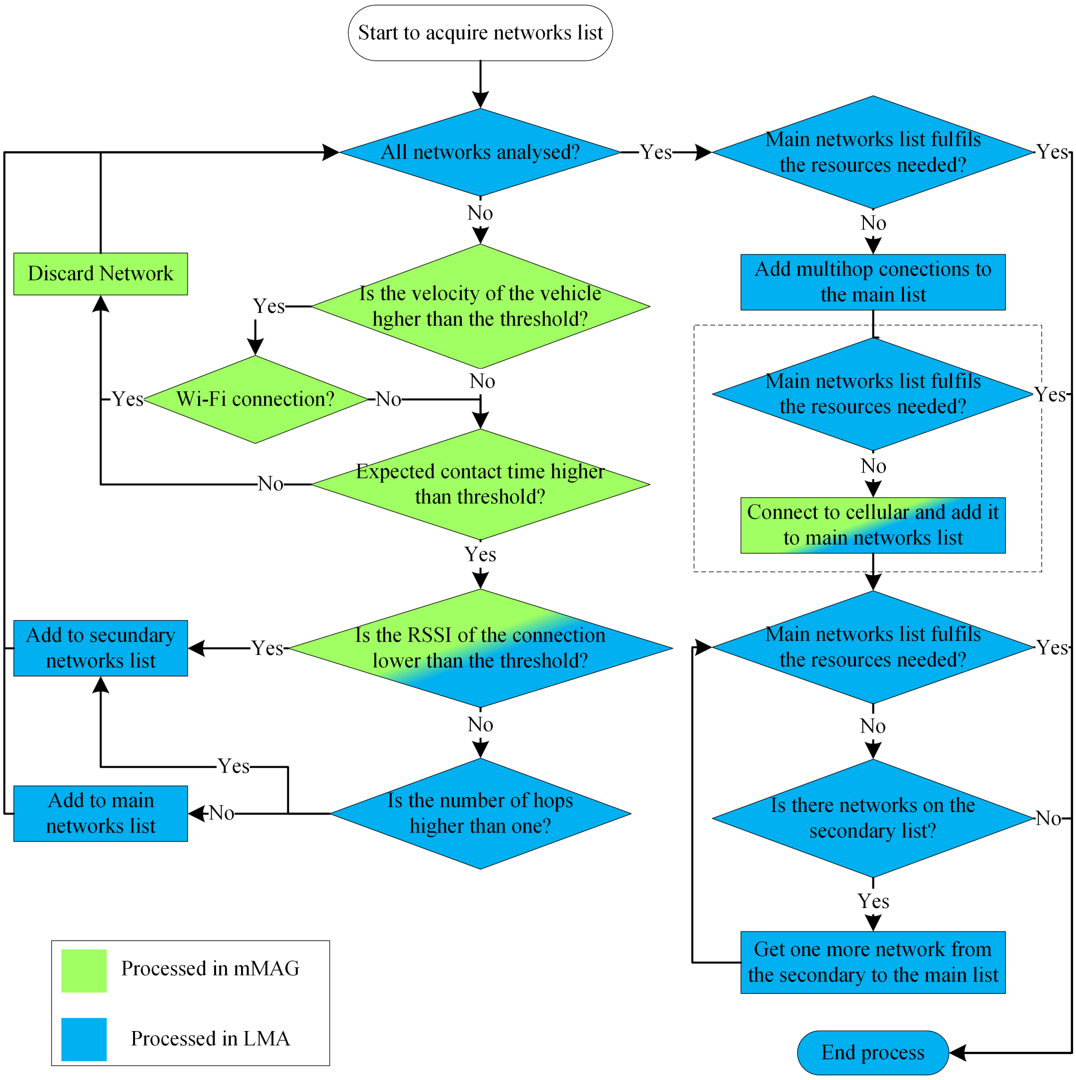


Figure 3.21: Operation flow of the distributed process of the constitution of the main networks list with the cellular addition

As the figure shows, the cellular is used in the case the main networks list does not fulfil the required needs for the traffic and the utilization of multihop connections is not enough either. In this case, if there is a non-allocated high priority traffic, the mMAG connects to the cellular network in order to fill that gap. This process is performed first in the mMAG that connects to cellular when it has no other good connections, and in the LMA side in which that connection is added to the main networks list. The non-priority traffic is stored in the mMAG and sent through opportunistic communications when a WAVE or Wi-Fi technologies are available.

3.7 Chapter considerations

With the actual state of VANETs, the mobility protocols are vast but the implementation is still not an explored field with little real world implementations. Given this fact, the N-PMIPv6 was chosen to be improved with multihoming in a vehicular environment. A multihoming implementation has been developed upon a similar protocol, PMIPv6, and the integration of both is the natural step in order to have a multihoming implementation in VANETs.

With an observation of both implementations and their operation, the integration was made in a way that some features of each solution were used to create the integrated one. Nevertheless, after the analysis of this integration, some improvements arisen related to the way multihoming can operate with WAVE, the needs in terms of connections managing and the possible improvements in the traffic distribution.

The broadcast nature of WAVE and the absence of session establishment allow the nodes to communicate to several other nodes without having to loose time when changing the PoA. This allows the multihoming to benefit from it, and one interface of the mMAG can be used to connect to several MAGs and create several paths to the LMA. For this, an adaptation of the way the LMA sees each path is needed so that one interface can have several registrations.

With multihoming, the management of the connections is important either in the LMA side, as in the mMAG connecting side. In this way, a connection manager is needed to connect and maintain more than one connection for each vehicle simultaneously.

The usage of this solution in the vehicular environment implies different restrictions to the usage of each connection in the way that the traffic should not be distributed in the same way as in the more static environments and with different needs. Consequently, a traffic distribution rule that takes into account the classification of the traffic and the qualitative classification of the networks is needed. This would translate in a more adequate usage of the network.

With this conceptual idea of the solution explained, one should take into account the more technical details that relate to this implementation. These details will be explained in the next chapter so that the implementation of this solution is fully understood.

Chapter 4

N-PMIPv6 and Multihoming - Implementation

4.1 Introduction

Although the concept of the developed solution was explained in the previous chapter, it is possible to observe it in a different perspective. Through the perspective of the implementation, it is possible to specify how it is developed and what are the technical details of this work. Therefore, this chapter presents the details of the implementation that allow the solution to work and perform according to the envisioned functionalities.

In this way, this chapter starts by explaining the details of the operative system that operates in the OBUs and RSUs. Thereafter, an analysis of the interoperation of the N-PMIPv6 and the multihoming is performed by giving an insight about the technical problems and how they were solved. In consequence, the details of the implementation and changes performed will be explained.

4.2 OpenWrt and VeniamOS

The equipment used as OBU and RSU is called NetRider and runs an operative system which is VeniamOS. This was built from an OpenWrt distribution [74] based on buildroot [75].

Buildroot is a group of Makefiles and patches that makes easier the generation of an embedded linux system. This also allows the use of cross-compilation for multiple target platforms through the cross compilation toolchain that is built, allows the generation of a kernel image and a bootloader image. Its use is mainly for small embedded systems that can be based on several architectures (such as the NetRiders).

This buildroot is used as basis for several other projects, including OpenWrt which is described as being a full-featured, easily modifiable and highly customizable linux distribution that is applied typically to routers. Allowing an easier packet management and changes, OpenWrt allows the developers to build an application without the need to work on the firmware related to it. In this way, OpenWrt is designed to be user friendly and provides an easy way of dealing with the packets for the NetRiders.

The operating system running on the NetRiders is the VeniamOS, which is based on the OpenWRT revision 35323 and includes some changes.

4.2.1 Build OpenWrt buildroot

In order to cross-compile programs to the NetRider architecture, an OpenWrt buildroot needs to be configured and built in a computer so that the application is built from there. Although the NetRider's Operating System (OS) is VeniamOS, this system is closely related to OpenWrt and the OpenWrt buildrrot will be enough to compile applications for this system.

Consequently, the most recent stable version of OpenWrt was installed. At the time of this installation, this version was 'Barrier Breaker' [76] that was released in October 2014 and supports several improvements to the previous versions, although they may not have been used in this dissertation. Besides, a new stable version of OpenWrt was released in September 2015, but the cross-compilation was not updated since it would not bring any advantage to the work performed.

The installation was performed following the tutorial provided by OpenWrt and presented in [77].

4.2.2 Basic OpenWrt operation

As explained before, OpenWrt is a set of makefiles that download, configure and compile packages according to the defined options.

It is divided into three main types of makefiles that are placed in three folders of the OpwnWrt main folder [78][79]:

- **Package:** This folder contains all makefiles that belong to the user-space tools and each tool has its own folder within this one, where it keeps the makefile and other optional files. These are the packages that the buildroot can compile and add to the target root file system.

- **Toolchain:** Here are situated the cross-compilation related software and makefiles like gcc, kernel-headers and others. This will also be responsible for the creation of the toolchain_dir (temporary directory for building the toolchain) and staging_dir (where the toolchain will be installed).

- **Target:** This is the place where the makefiles related to the generation of the target root file system image and the linux kernel are kept. There is a support for two types of file systems: jffs2 and squashfs.

It is also important to name the *dl* folder, where all the downloaded tarball files will be stored. These files correspond to the ones used in the packages and the target makefiles.

The operation of the main makefile is described by the following steps once the configuration is done [78]. These steps are executed when the *make* command is executed.

1. **Create the download directory ('dl'):** This is where the tarballs will be saved after they are downloaded, and where they will be kept so that they will not be downloaded everytime their compilation is needed.

2. **Create a build directory:** this is where the user-space tools (the ones whose makefiles are in the package folder) will be compiled.

3. **Create the toolchain build directory:** This is the place where the cross-compilation toolchain will be compiled.

4. **Setup staging directory:** This is where the previously compiled cross-compilation toolchain will be installed.

5. **Create the target directory and the target file system skeleton:** it will contain the final file system root.

6. **Install the user-space packages and finalise the image creation:** Install those packages into the root file system and compress it into the right format, placing the final firmware image in the 'bin/' folder.

4.2.3 Add a new package

One of the things that OpenWrt attempts is the easy portability of software. The package folder that corresponds to a certain tool can usually have three elements: Makefile, patches and files. The 'patches' contains bug fixes and optimisations, while the 'files' includes default configurations or initiation files, and these two items are optional. The really important item here is the Makefile, that contains the instructions for the download and compilation of that package.

The general appearance of this Makefile is completely different from a traditional Makefile, since this template has been created in order to reach into a more object oriented approach. With this, the abstraction is really higher since the majority of the operations performed are done in another Makefiles. Here the user will just need to specify a few variables.

First of all, in this Makefile, after the inclusion of the 'rules' file, the packet's source needs to be stated, specifying its information and download details. After this specification is performed, the description of the *package*, *menuconfig* and *ipk* entries need to be established so that the Makefile can identify the response to the input arguments passed to buildroot. Finally, it is also important the definition of the dependencies. A further explanation about this matter, about the structure of this Makefile and all the possible options can be found in [80].

In this way, in order to create a new package, a new folder is named after the application needs to be created within the 'package' folder, that contains the Makefile described above. Also, an Uniform Resource Locator (URL) needs to be specified that indicates the source code, or that source code needs to be inserted in the 'dl/' folder. Afterwards, this package must be selected in the menuconfig, and only compiled afterwards with the "make package/<path/to/the/package>/compile" command.

These were the steps that allowed the creation of the 'vmhpmip' package that is cross-compiled into the NetRiders. Also, in order to fulfil this compilation, the libfreeradius-client [81] library version 1.1.6, the ndisc6 [82] tool version 0.7.1, libpcap library [83] and libnetfilter_queue library [84] were added into the buildroot. These packages are used for authentication, neighbour IPv6 discovery, packet capture and queued packets usage, respectively.

4.3 First integration of multihoming framework and N-PMIPv6

In order to join together the multihoming functionalities to the N-PMIPv6 operation, there was a thorough examination of this integration. Several technical problems had to be taken into account:

- **Byte order:** The implementation of the multihoming architecture was performed in a way that all the nodes on the network were running in computers with the same byte order. The byte order problem is a well known one that can be summarized as follows: the storage of the bytes of one variable can be done from the most significant one, in lower address of memory, to the least significant one, in higher address of memory, (big endian) or the other way around (little endian). As there is no consent in what byte order all devices should use, there are implementations of both depending on the manufacturer option. Consequently, a conversion needs to be done to guarantee that the device is reading the data correctly.

  As a solution, since the accepted byte order to use in the network is big endian, every time one node sends information to the network, that information should be sent in big endian and upon the reception, a little endian node should perform the conversions. To support this conversion, the GNU C Library provides with functions to convert variables from network order and to network order, namely htonl (host to network 32 bits), htons (host to network 16 bits), ntohl (network to host 32 bits) and ntohs (network to host 32 bits).

  In this way, this operation is performed with the aid of those functions. But there is still a problem to be solved: the transmission of a double type variable which is stored as a floating-point number format. In this case, the double will be multiplied by a precision value that is usually with the format 10^x before the transmission, sent in an integer type and will be divided into a double variable when it is received. This process is described in the figure 4.1 where a big endian host (the vehicle) sends a double value to a little endian host. The double value is a floating point number,

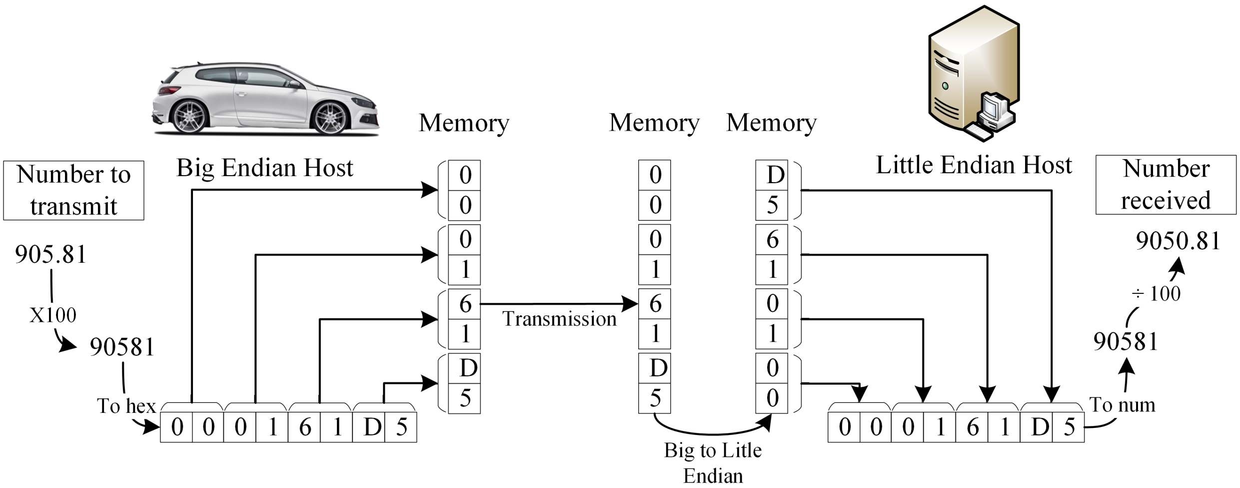


Figure 4.1: Sending a double from a big endian machine to a little endian one

and as its behaviour is not well defined in what regards endianness, the value is sent through an integer variable.

- **Integers type length:** Again, depending on the platform in which the program is running, the sizes of normal integer variables can be different. In this way, the messages exchanged will use the fixed length integers defined in the <stdint.h> file, so that its length will not be affected by the change of platform.

- **Broadcast RS message:** With the integration to the WAVE technology, the RS messages are sent by default in broadcast to every node at reach, which may pose a problem since the mMAG wants to connect to a specific MAG/mMAG. This would not happen with the traditional Wi-Fi technology, since it has a previous session establishment and these messages will only reach the devices to which the session is established with.

  In order to overtake this problem, a solution was already presented in the previous implementation of N-PMIPv6 [4] that allows the connecting mMAGs to send the RS to the specific device that it wants to connect to. In this way, the message is sent by the connection manager to the link-local address of that device, which is obtained through the MAC address announced when it announces the network.

- **N-PMIPv6 and multihoming authentication:** The original operation of PMIPv6 uses freeRADIUS system [85] to guarantee the correct authentication of the mMAGs. This system has a server that operates in the LMA and a client that operates in the MAGs, and when a mMAG connects to the MAG, this sends a message to the LMA that responds with another message in order to authenticate, or not, the mMAG.

  In an effort to minimize the messages exchanged, in the joint solution implemented here, the freeRADIUS usage was substituted for an alternative that was already provided by this PMIPv6 implementation. This alternative was the usage of a 'match' file instead of the use of freeRADIUS system, which is placed in the MAGs and contains information about the MAC address of the allowed interfaces.

4.4 One interface multihoming

As explained in the previous chapter, the improvement of using one interface to support more than one connection to the network was performed here. In the LMA side, this support implies the change in the way it identifies each BCE entry. This identification was extended with the use of the serving MAG address, which can be the MAG or mMAG to which the concerned mMAG is connecting to.

The BCE is supported through the implementation of a hash table which is a structure used to implement an associative array that can map keys to values. The mapping is normally performed through a hash function that calculates the position of a certain value in a series of buckets, based on one certain key. Therefore, the keys primarily used from the PMIPv6 implementation were the LMA address and the mMAG MAC address, and the value that corresponded to each key was the BCE entry that had all the information needed to the identification and characterization of the mMAG interface.

Consequently, in order to support the recognition of multiple connections of one interface, the BCE key needs to use one more parameter, the serving MAG address. Therefore, this address will be used in all the operations that involve the use of one BCE entry in the LMA:

- **Creation:** If the number of provided addresses is three, then the entry will be configured to use the new hash identification and calculation with three addresses as key. As a normal operation of this hash table implementation, if an address already exists with the same key, the new address will be added in the end of a linked list of the existent ones with that key.

- **Access:** The access is performed with the three addresses to calculate the key. The entries to which the hash function returns the same value are, as in the initial implementation, stored in a linked list under that bucket. These entries under the same bucket are then covered until one of them matches the three addresses of the key.

- **Deletion:** The deletion is also performed taking into account the three addresses of the key, and the same process as to access the entry to delete.

The way the BCE key is used in the hash function is through the division of each address into four sets of four bytes each, and then through a 'xor' of all those four bytes sets. Finaly, the rest of division of the result by the number of buckets where the BCE entries can be stored gives the number of the bucket where the BCE entry is stored. The operation of the hash table to learn the position of one BCE entry based on the addresses used as keys is represented in the figure 4.2.

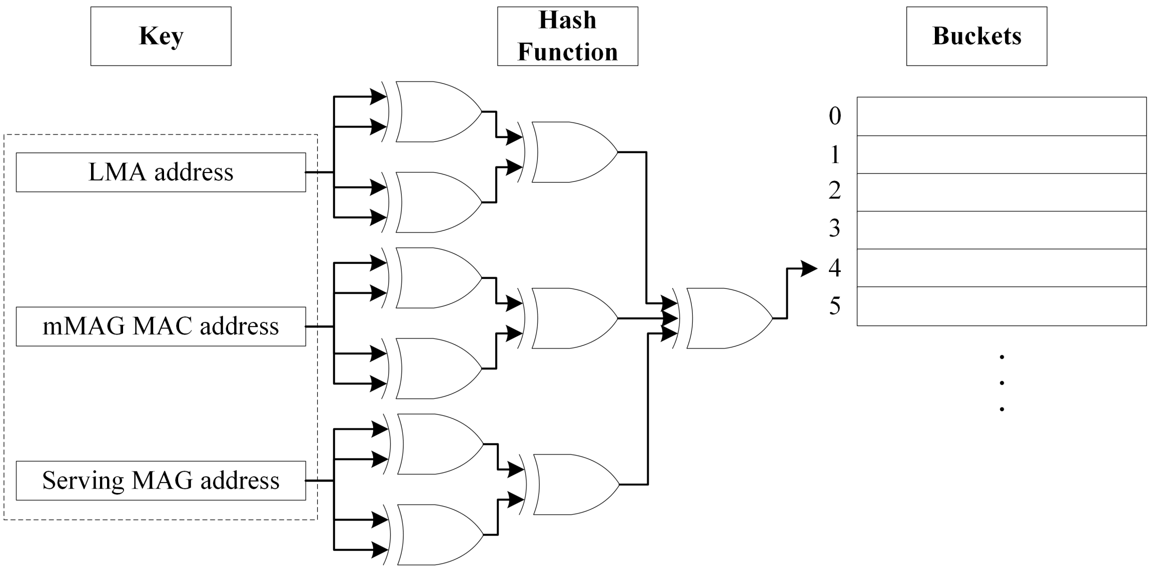


Figure 4.2: Operation of the hash table that uses the keys to get the correspondent position of the BCE entry in the buckets list

4.5 Multihoming connection manager

The connection manager implementation is divided into three main parts as explained in the previous chapter. These main parts are the Wi-Fi operation, WAVE operation and the reception of RAs. Each of these main parts is constituted of one thread, and one more thread was implemented with the aid of a parallel dissertation work that allows the ordered presentation of the recovered data an the used connections. In this way, the implementation of the three main parts of the connection manager will be explained. Note that this connection manager is integrated with the one of the parallel dissertation to include the cellular interface.

4.5.1 Wi-Fi operation

As explained in figure 3.11, the first step to perform a scan in the Wi-Fi networks is the verification of the velocity. This is performed through the utilization of a GPS unit that will provide with various data including the velocity with the command '*iw wave getlocalgps*' which uses an extension to the *iw* utility [86].

The next worth noticing block is the verification of the quality of the connection. To perform this verification, the file that states the statistics of the connection is read and its content is analysed. This file's contents are depicted in the figure 4.3 which belong to the the '/proc/net/wireles' file, and its contents identify several data for each interface named in the beginning of each line, including the quality of the link. This value is the one used to verify if there is the need to perform another scan or not.

Next, the scanning process is explained. This process uses the *iw* sockets and some more

```
Inter-| sta-|   Quality        |   Discarded packets               | Missed | WE
 face | tus | link level noise |  nwid  crypt   frag  retry   misc | beacon | 22
 wlan1: 0000    0     0      0        0      0      0      0      0        0
 wlan0: 0000   59.  -51.  -256        0      0      0      0      5        0
```

Figure 4.3: Contents of the '/proc/net/wireless' file

tools from the wireless tools package that are provided by linux in order to get information about the surrounding networks that are perceived in the mMAG, namely 'iw_get_range_info' to get data to use in 'iw_scan' which performs the scan of the available networks. Then, going through the data obtained, the best Wi-Fi network is selected, based on the RSSI.

Finally, concerning the RS transmission, this operation is performed through the rdisc6 program in the previous N-PMIPv6 implementation, and through the linux network manager in the previous multihoming implementation. In this case, none of the previous solutions can be taken. The rdisc6 could not be used because we need to send the information about the RSSI in the RS message, and the multihoming approach is also not possible since the OBU is not equiped with such software, and neither it would be plausible for the same reason as in the rdisc6.

In this way, when sending a RS message, a socket is used, the message is filled with the desired parameters and is sent to the link local of the MAG or mMAG to which the connection is desired. The connection manager takes advantage of two of the four reserved bytes of the RS message structure to send information about the RSSI. As it is visible in the figure 4.4, which presents the structure of the RS message, those bytes will be used.

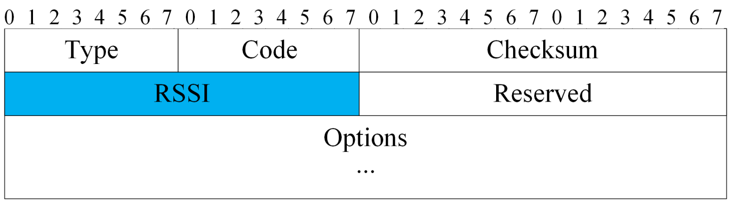


Figure 4.4: Structure of an RS message, based on [87]

Moreover, the MAC address of the PoA is maintained, so that the connection manager knows which is the network to which it is connected. This allows the connection manager to send periodic RS messages to the connected PoA.

4.5.2 WAVE operation

Regarding the WAVE operation, the flow described in the figure 3.12 has also some issues that worth noticing about its implementation.

The first one is the scanning process. This is done differently from the Wi-Fi scan, since it uses an *af_wme* type of socket. This was built in another extension that allows the scan of the networks with the IEEE 802.11p technology and uses defined structures to store the information. This scan is then performed in a way that, at every network iteration, the connection manager chooses if that network is worth connecting or not, based on its RSSI and expected connection time.

If the connection manager chooses one network to connect, if it is time to send a periodic RS, or if the connection manager senses a low RSSI and thinks it is disconnecting from that network, it sends one RS in the same way it is sent in Wi-Fi, a socket is created and the structure depicted in the figure 4.4 is filled up sending the message to the desired PoA.

Moreover, an array with the chosen and connected networks is maintained in order for the connection manager to know what are the actual connections and the time they were lastly verified. In this way, the connection manager can maintain the periodic RS message if they are at reach, and will erase them from the array if the network is not seen during a timeout time. This array contains the identification of the PoA through the MAC address, the timing information about the RSs and a flag that informs if a message with low RSSI was sent. In the case this message has been sent, the connection manager will stop the RS transmission to that network until its RSSI reaches a good RSSI level again.

4.5.3 RAs reception

Finally, in the messages reception, a raw socket is used to sniff the packets that reach the mMAG's interfaces. This socket is used instead of the PCAP tool, because this tool is not compatible with the IEEE 802.11p interface. The sniffing is performed in a way that the connection manager receives all the IPv6 packets, but it filters them so that it will only analyse the ones with the type 58 (Internet Control Message Protocol version 6 (ICMPv6)) and with ICMPv6 type 134 (RA).

Moreover, after the packet analysis, the prefix is taken and the IPv6 is built with the EUI-64 sufix as described in the figure 4.5. This IPv6 is then configured in the respective interface if it was not one of its IPv6 addresses yet.

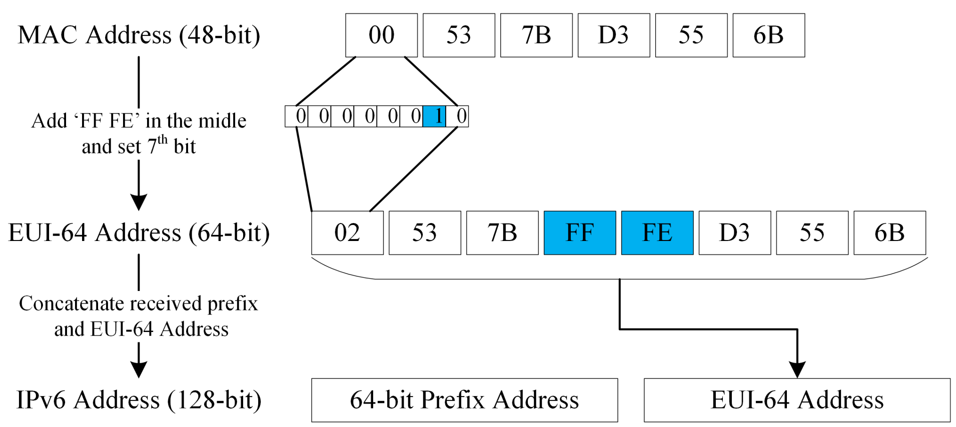


Figure 4.5: Construction of an IPv6 Address with the EUI-64

Also, after the registration of the connection, the routes are verified and if there are no connections in WAVE and cellular is not needed (no priority traffic and velocity of the vehicles is low), the route goes through the Wi-Fi interface if the RA was received there. Otherwise, if the RA was received in WAVE, the route is guaranteed to be through there.

Moreover, when the RA is received in the WAVE interface, a management is performed to the array with the connections, so that this connection will be added there, or if it exists already, their times updated.

4.6 Mobility and multihoming rule

The new calculation process of the rule is divided into some smaller sections. These sections are the flows identification and ordering, information retrieval and networks classification, and traffic division determination and distribution of groups and flows. These will be the addressed topics in this section.

4.6.1 Flows identification and ordering

The identification and ordering of the flows is performed in several steps. These steps and their details are specified below:

- **Identification:** The identification of the flows is performed right away when the LMA receives the first packet of that flow, and it is done through the verification of the port used by the flow. This port represents the group of traffic to which the flow belongs and allows the correct placement of the flow in the FCE.

- **Detect the place of insertion in FCE:** Knowing the group to which the flow belongs, and consequently its priority, the LMA goes through the FCE checking if it finds a flow with lower priority than the one being added. If it does find one, that is the chosen place (before the flow with lower priority and after the ones with higher or equal priority), but if it does not find, the present flow will be placed in the end of the array. One should notice that, if the priority level is the lowest, the array will not be covered since the place of the flow will be the last one anyway.

- **Insertion in the correct place:** Once the place of the flow is known, the ones that are in that place or with lower priority will be shifted so that the flow will fit in that place of the array. Furthermore, when placing a new flow or deleting an old one, the place of the last flow of each group with equal or less priority will be stored/updated, so that it can be used in the analysis of the groups.

4.6.2 Information retrieval and networks classification

Regarding the information retrieval in the LMA, the implementation changes the previous operation in one general aspect related with the sequence of the analysis. In the previous implementation the analysis was performed network by network, meaning that the request for information would be done for one interface and then the analysis to that network would be performed. Here this is changed, the LMA asks for information about every MAG before processing any of the information. This is done because the analysis will now take into account data from other networks too (this point will be further explained in section 4.6.3).

The information needed by the LMA to classify the networks and calculate the rule comprises the statistics of the MAG and the information about the connection between the MAG and mMAG. The MAG statistics retrieval remains the same as in the base implementation of multihoming, comprising data about intput and outpud mean packet size (mps) and packets per second (pps) (through the retrieval of information of the */proc/net/dev* file); but the retrieval of the information of the connection was completely changed. The part of that information that is used to the rule calculation is estimated in the LMA instead of coming from the MAG.

Furthermore, there are still two parameters which their retrieval was not mentioned in this section: the technology and the RSSI. The technology is used not only to the new calculation of the Achieved Throughput (AT) (explained in section 4.6.3), but also to consider the allocation of the flows to the best networks, and the RSSI is used to create the list of best networks. In this way, the technology information arrives in the existent PBU option, and is stored in the BCE and UCE so that it can be used any time. In the other side, the RSSI information is stored in the MAG everytime it receives a RS and is sent to the LMA with the message that contains information about the MAG to the rule calculation. For a low RSSI, the mMAG informs the MAG with a RS right away (without waiting for the periodic one) containing that value, and the MAG sends an information message to the LMA containing the RSSI which will trigger a recalculation of the traffic division, where this network will be accounted in the secondary networks list.

The creation of the selected networks list is explained in the figure 3.18 and its implementation is performed, from the mMAG side, in the connection manager and, from the LMA side, after the information retrieval and before the calculation of each network's data.

4.6.3 Traffic division determination and distribution of groups and flows

First of all, in what regards the estimation of the real characteristics that were before obtained through the modified version of the Wbest, the part of that information that is used to the rule calculation is now determined in the LMA with the following recipe for the calculation of the AT, based on the capacity of the MAG and its load:

$$\mathrm{AT} = Capacity - \mathrm{PoA}TotalLoad \tag{4.1}$$

In this recipe, the capacity is the defined for each PoA and its total load can be calculated with information about its input and output pps and mps obtained from the MAG. The calculation of the AT between the MAG and the mMAG is therefore determined as according to the equation 4.2.

$$\mathrm{AT} = Capacity - (\mathrm{pps}_{input} * \mathrm{mps}_{input} + \mathrm{pps}_{output} * \mathrm{mps}_{output}) \tag{4.2}$$

As depicted in the figure 4.6, the output is the traffic that flows out of the PoA and the input is the traffic that is received in this same PoA. As the figure shows, this traffic has a particularity when using WAVE technology due to its broadcast nature and operation in the same channel. When the PoAs can see each other, the output traffic sent through each one is seen as input to the other one. The influence of this specific aspect is analysed next.

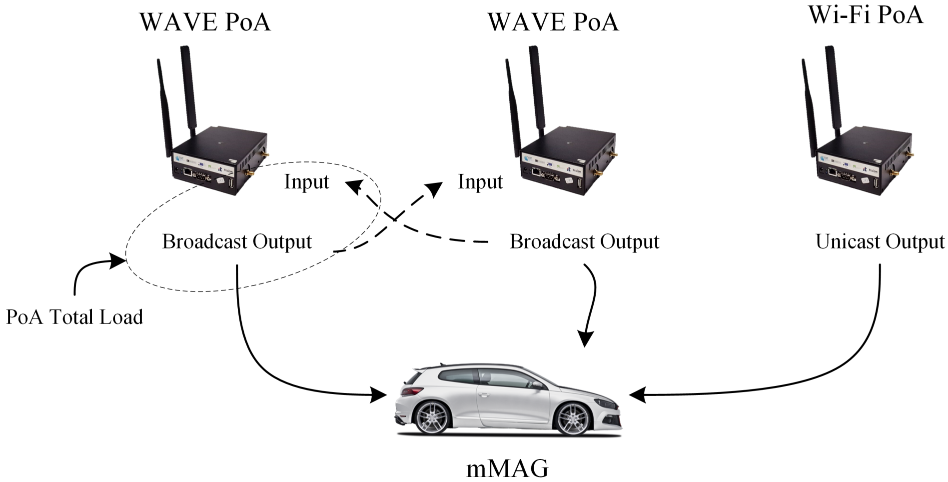


Figure 4.6: PoA load seen as the sum of the input and output traffic in each PoA and the inter-PoA influence

The determination of the AT allows the consequent calculation of the AT without the multihoming traffic impact. This value is important for the determination of the optimal division rule. The traffic that is going through the MAG and which is aimed to this mMAG, should not be considered in the calculations since it would affect the final value. In other words, the part of the MAG load relative to this mMAG should be considered null for the calculations so that the real free capacity would be obtained. The percentage is applied to all the mMAG traffic and not only to a part of it. In this way, the base implementation of multihoming used to calculate the AT without the multihomng impact is performed by adding to the AT the percentage ($percentage_{this}\mathrm{PoA}$) of the mMAG traffic ($\mathrm{pps}_{mMAG} * \mathrm{mps}_{mMAG}$) that was allocated to that MAG. This calculation is shown in equation 4.3 and is still the one utilized to non-WAVE interfaces.

$$\mathrm{AT}'_{non-WAVE} = \mathrm{AT} + \mathrm{pps}_{mMAG} * \mathrm{mps}_{mMAG} * allocated\%_{this}\mathrm{PoA} \tag{4.3}$$

But with the use of WAVE and the improvement to perform multihoming on one interface, if the PoAs where the MAGs are placed see each other, then they will sense each other's traffic (as seen in figure 4.6). In this way, the previous manner of eliminating the traffic to the mMAG in order to perform this calculation will not be enough, and an improved solution needs to be implemented. Then, for the case in which the MAGs see each other, the calculation of the AT without this traffic impact (AT') for WAVE PoAs should take into account each other's traffic being the following recipe applied:

$$\mathrm{AT}'_{wave} = \mathrm{AT} + \sum_{i \in WAVE} \mathrm{pps}_{mMAG} * \mathrm{mps}_{mMAG} * percentage_i \tag{4.4}$$

In this way, although the AT' for Wi-Fi and cellular takes only the traffic of that MAG into consideration, the AT' for the WAVE interfaces takes into account the traffic sent to the other WAVE MAGs if they see each other, in order to discount the traffic that corresponds to the actual mMAG from the PoA load under analysis.

In this way, this information, and the remaining obtained is used to calculate the optimized division of the traffic. This calculation uses a modified version of the genetic algorithm from the multihoming implementation that served as base for this work. The modifications to the algorithm regard the fact that the medium through which the MAGs are sending traffic is the same. As seen in the figure 4.7, although the sum of the capacities of the WAVE PoAs can be larger, the real limitation is imposed in the load that the medium can take. Then, if each WAVE PoA is limited to 'X', the sum of the throughput that they can send to the mMAG is at maximum 'X', because 'X' represents the traffic it can send if it is using the medium all the time. As each MAG will have to divide the medium with the other MAGs (assuming they are seeing each other), it will only be able to send traffic during a portion of the time. In this way, and as it is assumed that the limitation of every WAVE PoA is the same, the sum of the usage of each one will be, at maximum, the limitation of one of them.

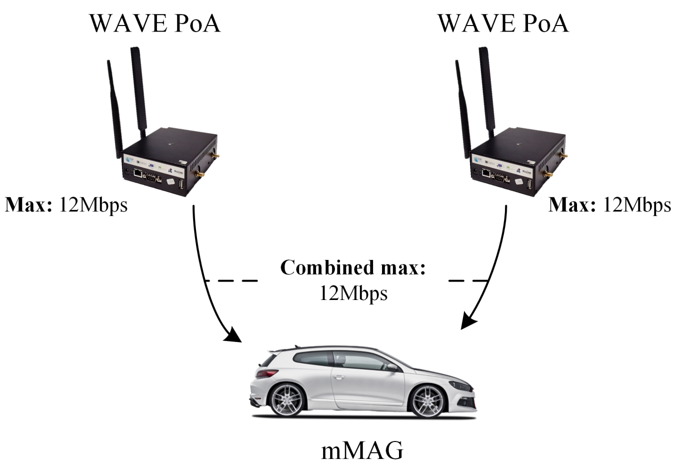


Figure 4.7: The rate limit imposed to the PoAs will be the limit of usage of the medium

In order to solve this problem, the genetic algorithm that calculates the percentages allocated to each MAG was changed with this limitation. The choice was taken in a way that, the usage of the WAVE PoAs is favoured due to the fact that the implementation is in a VANET and the technology is adapted to that environment. The changes to the genetic algorithm were then made in the way that, even considering the AT' of each PoA as the maximum to one single PoA, the sum of the traffic allocated to the WAVE ones is limited to the AT' of one of them (since we are considering that the MAGs will see each other and compete for the same medium access). This approach will maximize the usage of WAVE because the algorithm will be led to distribute the traffic according to the maximum AT' of each PoA, but will only be limited if the sum surpasses the limit.

Regarding the implementation of the distribution of the groups of flows described in the section 3.5.3, the first verification is about their accommodation in one path and is done through the comparison between the total traffic of that group (obtained by the sum of the multiplication of the pps by the mps for each flow of that group) and the percentage of the total traffic allocated to one network, taking into account the previous allocations. As described in the equation 4.5, the group will fit in that network if the left operand (throughput occupied by the group) is smaller or equal to the right one (free percentage of the traffic allocated to that network).

$$\sum_{flow \in Group} \mathrm{pps}_{flow} * \mathrm{mps}_{flow} \leq nonAllocated\%_{network} * \mathrm{pps}_{mMAG} * \mathrm{mps}_{mMAG} \tag{4.5}$$

In this case, the pps_{flow} and mps_{flow} are obtained in the LMA through the monitoring of the packets of each flow, and the sum of these values for the flows of one mMAG will result in the pps_{mMAG} and mps_{mMAG}, respectively. On the other side, the $freePercentage_{network}$ is the total percentage allocated to one network subtracted by the part of that percentage already allocated to other flows/groups.

Upon this verification, if the group does not fit in one network, the LMA will try to accommodate its traffic flow-by-flow in the available networks. To verify if the available throughput in one network is enough to accommodate one flow, the throughput of the flow is compared with the percentage of the total traffic allocated to the network, and to verify if it surpasses the optimal percentage allocated in a large value, a limit is established which is a portion of the percentage allocated to the network. As an example, if the percentage of traffic allocated to the network is 30%, and if that portion is defined as 10%, one flow will be accepted in this network if the percentage of the network previously occupied plus the percentage that corresponds to the flow does not surpass the $30\% * (100\% + 10\%) = 33\%$. This situation is described in the equation 4.6.

$$allocated\%_{network} + \%_{flow} \leq \%allocated_{network} * (100\% + extraPortion) \tag{4.6}$$

In order to have success with this approach, the best network calculation is crucial. This is done several times along the process, because, when some traffic is allocated to one network, it decreases its available non allocated percentage of traffic. This traffic not allocated starts with the optimal value, given from the algorithm that minimizes the time of the packets in the network, and decreases to zero when the network is full. Hence, he best network calculation takes three factors into account:

- Network is on the **main networks list**, not being accounted for, if it is not accounted there.

- **Access technology** is an important factor and the WAVE technology is the one that is prioritized. The WAVE networks will be firstly considered for the best and the others will only be considered if the WAVE ones are filed up. In this way, if it is not a WAVE network, the priority traffic will go through cellular, and the less priority traffic or one flow that does not fit entirely in one of the WAVE networks goes through Wi-Fi if it is available (if not, it stores the information until a connection is available).

- The network with the **bigger non allocated percentage of traffic** is the one chosen. When allocating flows or groups to one network, the best one may change because the free percentage that this network can still accommodate becomes lower.

Lastly, when each packet is being analysed, a verification is performed to see which is the situation of the group and flow to which it belongs. As described in the algorithm 1, if the group or the flow is allocated to one of the networks it will be directed there and, if it is not, an algorithm based in the base implementation of multihoming is used to distribute the packets to the available space in each network.

This algorithm calculates a random value between one and the sum of the available space in the networks' allocated percentage, if that packet belongs to the less prioritized group, and between zero and the percentage of the flow if the packet belongs to a flow that was distributed through more than one network. The network which percentage wraps that value if the percentages are concatenated, is the selected network to send the packet. As an example, if there are two networks that comprise 10% and 15% of the total traffic respectively, the packets with a random value from 1 to 10 go through the first network and from 11 to 25 go through the second one.

4.7 Chapter considerations

The implementation of the solution described in the chapter 3 is comprised of several parts, namely the creation of a package to enable the utilization of VeniamOs, the primary integration of N-PMIPv6, and the multihoming and its operation in the NetRiders, the implementation of multihoming with one interface, the implementation of the connection manager and finally the adaptation of the traffic distribution rule.

With the creation of a package to work with the NetRiders, a cross-compilation platform had to be used. This platform is an openWrt buildroot wich is based on the buidroot. A package was created that allows the cross-compilation to the NetRides system.

Algorithm 1: Distribution of each packet by the networks, derived from [7]

```
if N_networks ≥ 1 then
    if assignedNetworks_group == 1 then
        Packet through that network;
    else
        if assignedNetworks_flow == 1 then
            Packet through that network;
        else
            AC = 0;
            if Group less prioritYzed then
                Rv = random]0, freePercentage_total];
            else
                Rv = random]0, percentage_flow];
            end
            for n ∈ Networks do
                if Group less prioritYzed then
                    percentage_n = freePercentage_n
                else
                    percentage_n = flowPercentage_n
                end
                if Rv ≤ (percentage_n + AC) and percentage_n ≠ 0 then
                    Packet through this network (n);
                else
                    AC = AC + percentage_n
                end
            end
        end
    end
else
    Send the packet through the only network
end
```

Regarding the primary integration of the N-PMIPv6 and multihoming, some constrains had to be taken into account, mainly related to the difference between the systems used to accommodate the LMA and the MAGs, and to the WAVE technology.

In order to implement the one interface multihoming, the registration of the mMAGs on the LMA had to be changed. In this way, a new part was added to the BCE key, the address of the serving MAG. This brought a new problem with the handovers that now cease to exist which is compensated by the operation of the traffic division rule and the connection manager.

This connection manager is used as the connecting entity for the mMAGs and is divided into three main parts that use tools from the linux wireless, and others that support the usage of Wi-Fi and WAVE technologies. Also, it sends information about the state of the connection to its serving MAG, namely the RSSI.

Moreover, regarding the adaptation of the traffic division rule, some changes are made in the retrieval of information about the network and also in the way the division of the traffic is performed. Some parameters are estimated to serve as input to the optimal division calculation and after that calculation, the flows are analysed by categories and allocated to go through one network if they fit there.

Being the solution and its implementation explained, its evaluation follows. This evaluation will analyse the changes made to reach the complete multihoming solution.

Chapter 5

Evaluation

5.1 Introduction

Upon the development of the mobility and multihoming solution, an evaluation is needed so that one can assess its performance in real networks. The aim here is to evaluate the actual solution and the improvements performed through tests to the several mechanisms implemented.

First of all, an evaluation is done to the basic features of multihoming that confirm the correct functioning and benefits of the implementation. Moreover, the changes performed are analysed to confirm the good performance of the implementation.

Section 5.2 explains the details about the equipment used in the testbed that allows the development and evaluation of this solution.

Section 5.3 goes into detail about the scenarios specification and the way they were used to perform the evaluation and obtain the results. The details of each experiment are described in this section.

Following the specifications, section 5.4 shows the results obtained from the implementation of the scenarios specified in the previous section. In this section a further analysis is performed to these results in terms of performance and functionalities.

In this way, this chapter presents the details about the equipment used in this evaluation, the tested scenarios and the obtained results.

5.2 Equipment

In order to build and implement a VANET scenario, there are several elements that need to be taken into account. As the network is constituted by vehicles, there is a necessity to have an OBU in each vehicle where the mMAG operates, and several RSUs alongside the road where the MAG operates to provide an infrastructural access to the internet and improve the connectivity of the network. OBUs and RSUs can have a similar hardware and software despite the different functions, and contain the following elements:

- **Central Processing Unit (CPU)** processes and runs the applications and the communication protocols;
- **Wireless transceiver** exchanges information between OBUs and between RSUs and OBUs;
- **GPS receiver** provides informations about location, velocity, direction and time synchronization;
- **Sensors** reads the information needed to send to other vehicles or to the network;
- **Input/output interface** provides human interaction.

The equipment that is used as OBU and RSU fulfils the previous requirements and is called NetRider®. It has multiple network interfaces so that it can communicate in a V2V or V2I manner. This equipment contains several elements [88], namely a Single Board Computer (SBC), DSRC wireless interface, Wi-Fi interface, cellular interface, GPS receiver and antennas for each device. It implements the WAVE latest standards and the relevant elements for this work have the following characteristics:

- **SBC with the CPU**:

  - Alix3D3 Module with a 500 MHz AMD Geode LX800, 32-bit x86 architecture, 59 MB of memory and Ethernet connection;

- **Wireless transceivers**:

  - mini-PCI 802.11p-compliant wireless interface with the Atheros AR5414 chipset that supports the ath5k driver;

  - Wi-Fi Module compliant with IEEE 802.11a/b/g;

  - Cellular interface.

- **Antennas**:

  - Omnidirectional antenna prepared for frequencies in the range of 2.4 GHz, with a 5dBi gain;

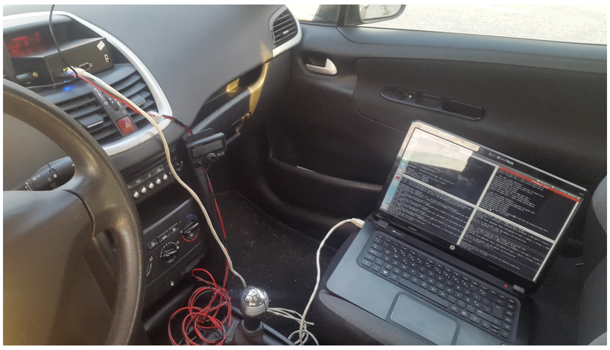
  - Omnidirectional L-Com Antenna used for frequencies between 5.850 and 5.925 GHz, with a 5dBi gain;

- **GPS receiver**:

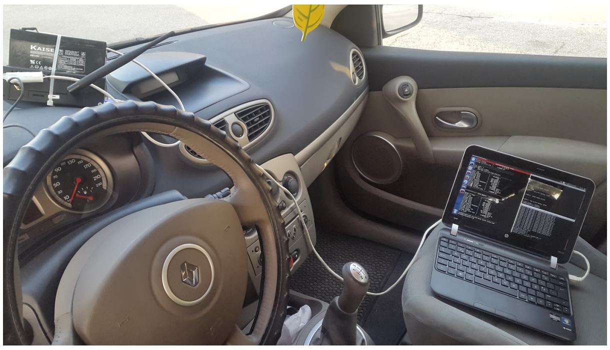
  - GPS GlobalTop (MediaTek MT3329);

Regarding the software, the NetRiders are running a tailored linux distribution based on buildroot [75], the VeniamOS v19.2.

An image of the OBUs inside the vehicles is presented in figures 5.1a and 5.1b. The RSUs are presented in figure 5.1c. Notice that another NetRider is also used as CN to generate traffic to the mMAG; this CN can be seen in figure 5.1d alongside the LMA.



(a) OBU 1



(b) OBU 2

(c) RSU

(d) LMA & CN

Figure 5.1: Testbeds used on the road

The LMA, shown in figure 5.1d, is a computer which has a cabled connection to the MAGs in the case of the lab scenarios, and is Wi-Fi connected to the MAGs in the road scenarios. The computer used here was a Samsung laptop. Table 5.1 depicts the details of the NetRiders and the computer characteristics.

Table 5.1: Characteristics of the elements of the network

Parameter	**NetRiders (OBU/RSU/CN)**	**LMA**
CPU	500 MHz	2 200 MHz x 8
Memory	59 MB	196,8 GB
OS	VeniamOS v19.2	Ubuntu v14.04
Linux Kernel	3.7.4	3.13.1

Furthermore, in the road scenarios, two vehicles were used in which the OBUs were placed. These vehicles were a Peugeot 207 in which the first mMAG was placed, and a Renault Clio III in which the second mMAG was placed to be used as the multihop node. These vehicles can be seen in the figures 5.2.

Figure 5.2: Cars used in the road experiments

5.3 Scenarios

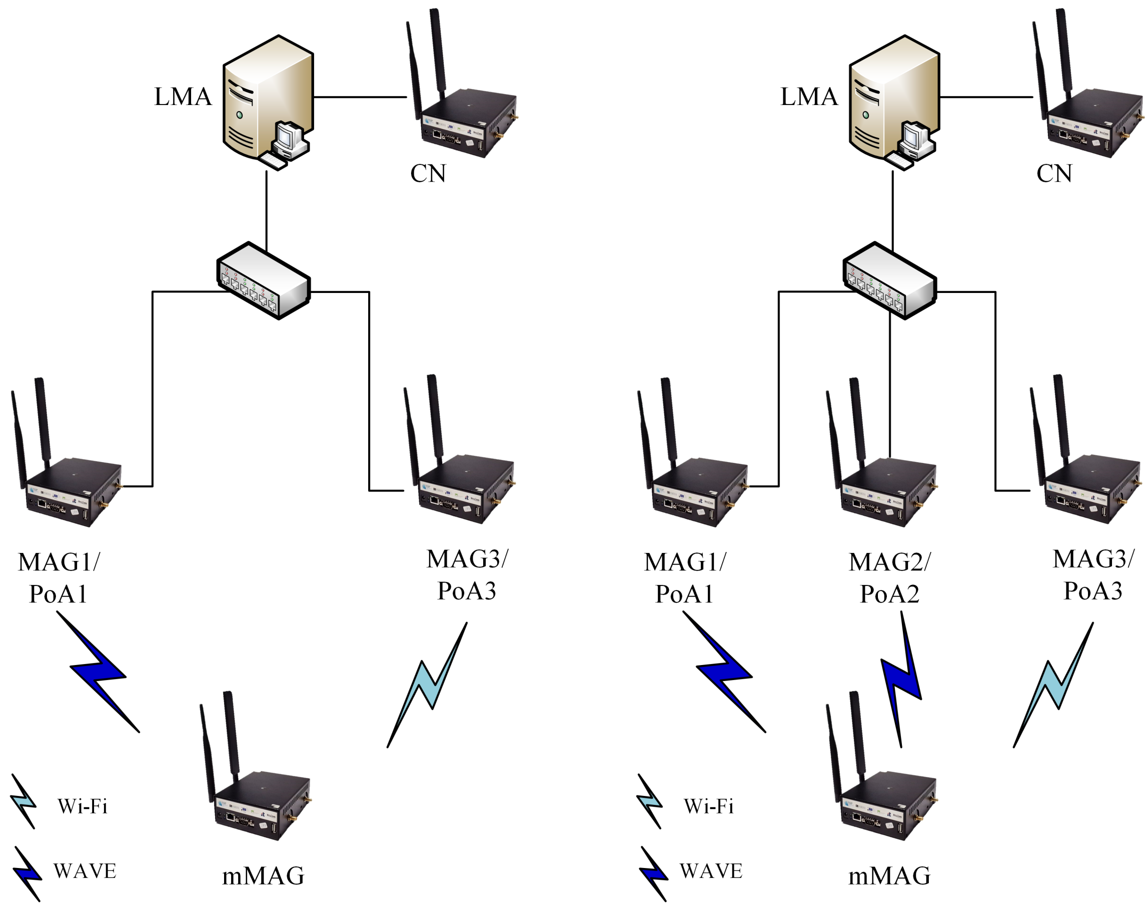
5.3.1 Laboratory Scenario

The first considered scenario is a laboratory one. This scenario has two variants depicted in the figures 5.3a and 5.3b, and it is based on a multihoming case with two or three MAGs working as RSUs. Here, the CN runs in a NetRider connected to the LMA through an ethernet cable. The LMA is also cabled connected to a hub that supports the connections to the MAGs and, finally, the mMAG has the possibility to connect to the WAVE PoAs and/or to the Wi-Fi PoA. In this way, the mMAG can operate in multihoming through more than one technology and/or through the same (WAVE). In this testbed, all entities but the CN run the multihoming implementation described in this document without the alterations performed in the parallel dissertation, and the mMAG is also running the implemented connection manager.

In these scenarios, the RSUs can provide WAVE and Wi-Fi PoAs. The WAVE ones are limited in a way that they will, in the maximum, reach 12.9 Mbps and the Wi-Fi one will reach 6.9 Mbps.

In this scenario several measurements will be performed to test different aspects of the implementation, namely aspects relative to the overall multihoming performance (throughput, delay, losses and PoAs load) and, more specifically, the aspects related to the optimized division rule (best percentage determination, adaptation of the rule, distribution of the groups and flows, improvement in the out-of-order packets and the overall time of calculation).

The traffic generation is always performed from the CN node with the destination of the mMAG, passing through the LMA and through the selected MAGs. The traffic used for this evaluation is always UDP, since the evaluation is aimed only to the downlink traffic.



(a) Multihoming through two PoAs (b) Multihoming through three PoAs

Figure 5.3: Testbeds used in the laboratory

5.3.1.1 Overal multihoming performance

In order to evaluate the performance of the multihoming implementation, the scenarios represented on the figures 5.3a and 5.3b were tested using the Distributed Internet Traffic Generator (D-ITG) tool [89] to create traffic during five minutes and analysing it in five seconds intervals.

The first metrics analysed are the throughput, packet loss and delay. These values are obtained through the examination of the connection in single path (through just one MAG) for every MAG used and for the aforementioned testbeds using four transmission rates:

- **3 Mbps:** Low rate that is supposed to be transmitted seamlessly in every case. This traffic is composed of two flows of 300 kbps for the most prioritized group (type 2), two flows of 600 kbps for the second most prioritized group (type 1) and one flow of 1.2 Mbps for the least prioritized group (type 0).
- **6 Mbps:** Higher rate that should get near the saturation of the Wi-Fi MAG in the single path scenario. This traffic is composed of two flows of 600 kbps for the most prioritized group (type 2), two flows of 1.2 Mbps for the second most prioritized group (type 1) and one flow of 2.4 Mbps for the least prioritized group (type 0).
- **12 Mbps:** Rate that should be transmitted in both WAVE MAGs, should not be fully transmitted in the Wi-Fi MAG and should fit in the multihoming scenario. This traffic is composed of two flows of 1.2 Mbps for the most prioritized group (type 2), two flows of 2.4 Mbps for the second most prioritized group (type 1) and one flow of 4.8 Mbps for the least prioritized group (type 0).
- **18 Mbps:** The single path scenarios should show saturated results and the multihoming scenarios would fit the entire 18 Mbps, differing only in the delay since the overall processing power is higher. This traffic is composed of two flows of 1.8 Mbps for the most prioritized group (type 2), two flows of 3 Mbps for the second most prioritized group (type 1) and one flow of 8.4 Mbps for the least prioritized group (type 0).

Relatively to the next measurements, they are about each PoA output load when in multihoming. These measurements will present a lower PoA load when the number of MAGs is higher. The addition of one WAVE PoA will not increase the total throughput in the network, since the WAVE interfaces of both RSUs use the same channel and directly interfere with one another, but it will allow a better load balancing due to the fact that each RSU will have less packets to process. The traffic introduced to these measurements is the same as in the previous case of the throughput, packet loss and delay.

5.3.1.2 Optimized Division Rule

Being the overall performance of multihoming verified, an insight was given into the traffic division rule mechanisms. This rule is firstly shown as the one that provides the best packet delay when using two PoAs with different technologies, adapting to the extra traffic. Afterwards, the distribution of the flows and groups of flows is verified and its improvement is shown in comparison with the static division that performs a promiscuous packet division. Finally, the time of calculation of the rule is analysed, taking into consideration each of its phases.

Best division

In order to verify the best division and its dynamics, the scenario of multihoming through two PoAs presented in the figure 5.3a was tested using the D-ITG tool [89] to generate traffic of 12 Mbps (two flows of 1.2 Mbps for the most prioritized group, two flows of 2.4 Mbps for the second most prioritized group and one flow of 4.2 Mbps for the least prioritized group) from the CN to the mMAG during five minutes and analysed in intervals of five seconds. In order to verify that the dynamically calculated rule is indeed the one with the best delays, two static divisions were also tested in the way that each one of them would differ in 10 percent from the mean of the dynamic one.

Relatively to the rule adaptability, a first test was performed with the scenario of the figure 5.3a, and then, traffic belonging to another mMAG was introduced in one of the PoAs (PoA 1), according to the figure 5.4. This allows to verify that the rule allocation will change according to the overall traffic and to the achieved throughput determined in the LMA for the mMAG under study. For this evaluation, 12 Mbps of traffic (two flows of 1.2 Mbps for the most prioritized group, two flows of 2.4 Mbps for the second most prioritized group and one flow of 4.2 Mbps for the least prioritized group) were also generated with the D-ITG tool in a period that fulfils 10 iterations of the rule calculation.

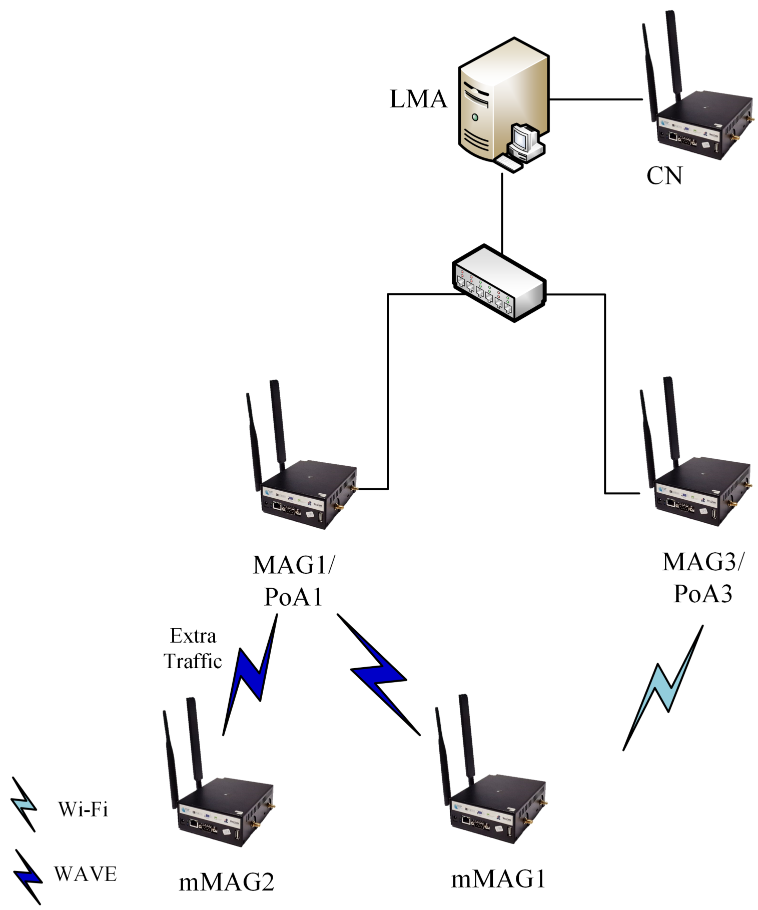


Figure 5.4: Multihoming testbed with interference from another mMAG

Group and flow division performance

One of the improvements in the multihoming implementation is the flows classification, grouping and distribution by the different networks. This improvement is shown through the usage of the several flows when the mMAG is connected through several PoAs. In this case, the scenario presented in the figure 5.3b is used and several flows are introduced which allow a good evaluation of this implementation. Here, the traffic is generated through the iperf tool [19], with five flows of 1 Mbps for the most prioritized group (type 2), five flows of 1.5 Mbps for the second most prioritized group (type 1) and two flows of 2 Mbps for the least prioritized group (type 0) are used, completing a total throughput of 16.5 Mbps. This measurement is performed in 10 iterations of the rule calculation and allows the verification of the division of flows and the observation of the priority given.

Still in the flows distribution, another measurement was performed that shows the influence of this feature in the out-of-order packets. As the packets of one flow are now going mostly through one path, the out-of-order packets are expected to be less than in the previous implementation without this feature. In the previous implementation, the different delays of two paths could lead to a more often occurrence of this phenomenon. In this measurement, four flows of 1 Mbps for each priority are sent using the iperf tool completing a total of 12 Mbps. In this case, the flows are all the same for every traffic priority because the point is to verify the improved service for the top priority when all the remaining features of the traffic are the same. The measurements are taken in three iterations of five minutes each.

Time expenditure

Lastly, the final measurement for this laboratory testbed is related to the time spent for the total rule calculation. This time includes all the tasks of the multihoming rule calculation:

- **initialization:** Preparation of the variables and memory allocation that supports all the process.
- **Information requests:** Request of information from the LMA's IM to the MAGs' NIS and response.
- **Calculations:** Processing of the information obtained from the MAGs in order to use it in the next step.
- **Algorithm:** Genetic algorithm that calculates the division rule.
- **Flows assignment:** Time that takes for the LMA to distribute the flows for this mMAG according to the percentages obtained in the previous step.
- **IP replication and data storage:** Transmission of the message that informs the mMAG to replicate its IP and storage of all the information relative to this process.

The time measurement is obtained through the generation of 12 Mbps traffic (two flows of 1.2 Mbps for the most prioritized group (type 2), two flows of 2.4 Mbps for the second most prioritized group (type 1) and one flow of 4.8 Mbps for the least prioritized group (type 0)) using the iperf tool. Ten iterations of the rule calculation are used in these results.

5.3.2 Road Scenario

A road scenario was also considered in order to verify the mobility and multihoming in a real vehicular environment. The scenario considered in the figure 5.5 was used to evaluate the tests in which a vehicle roams from a place where it has only one RSU at reach to a place where it can be connected in multihoming to two RSUs, and next to a place where it will only be connected to the second RSU. In this scenario the RSUs are spaced by 85 meters. Figure 5.6 presents the scenario used in these tests that can be devided in two: single-hop, where the second mMAG is not connected and the traffic is generated to the first vehicle; multihop, where the second mMAG is connected to the first one and the generated traffic has the destination of the mMAG 2. In this testbed, the CN is connected to the LMA through an ethernet cable, which, in its turn, is connected through Wi-Fi to the MAGs (the ethernet cable is not feasible since it would have to be very long). Also, the first mMAG connects to the MAGs through WAVE technology and the second one, when used, connects to the first mMAG also through WAVE technology.

Figure 5.5: Route covered by the vehicle

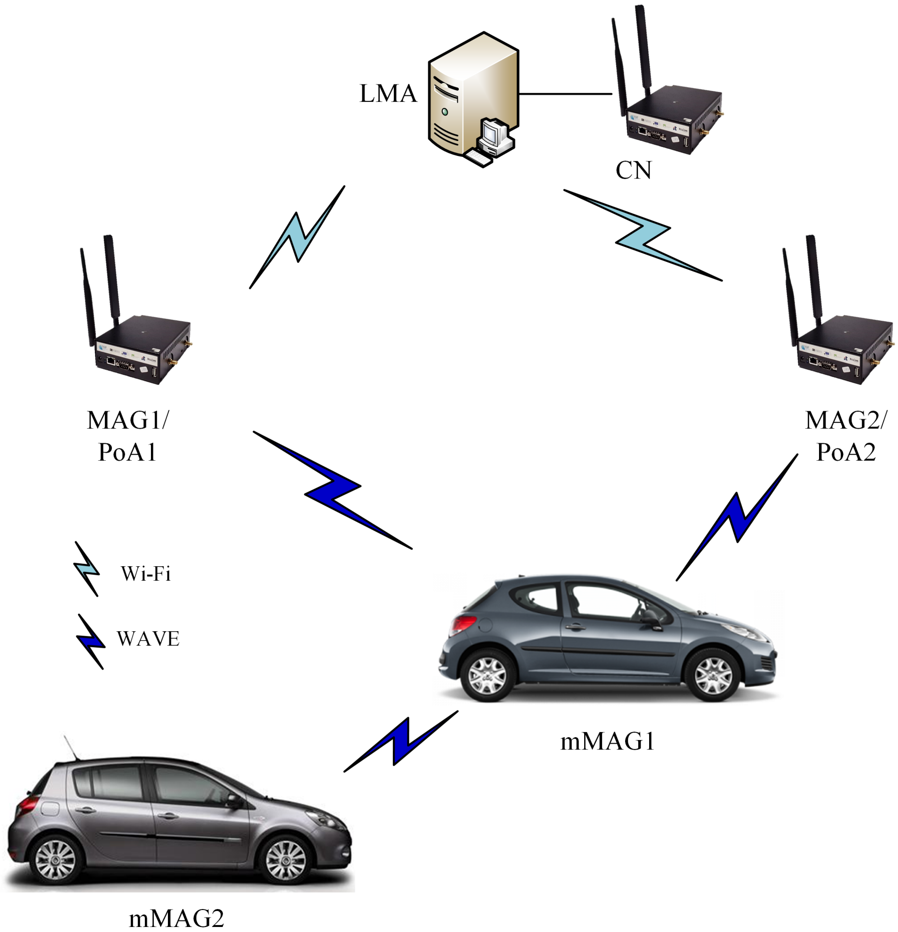


Figure 5.6: Scenario used in the road tests

All entities, except for the CN, run the implementation described in this dissertation joint together with the changes performed in the parallel dissertation. This implementation's features are described in the section 3.6 of this document.

Relatively to the rate, just as in the laboratory tests, the WAVE PoAs are limited to 12.9 Mbps each, and the range of each one reaches the other one, being the WAVE traffic of each one seen by the other. On the other side, the connection between the LMA and the RSUs is made through Wi-Fi at a relatively long distance and, therefore, the generated traffic in these experiments will be of 500 kbps in order to minimize the packet losses in those links. One traffic flow with this rate will then be generated with the D-ITG tool from the CN to one of the mMAGs depending on the scenario.

These tests are aimed to verify the mobility mechanisms in a real road scenario and are divided into two phases:

- **Single-hop:** In this phase, the situation shown in figure 5.5 in which the vehicle roams from one point to another passing by the RSUs is tested. This will evaluate the implementation of the connection and disconnection of the mMAG from one MAG. As the implementation of the disconnection message in this dissertation was performed, as a proof of concept, through the same MAG from which it is disconnecting, the high velocity of the vehicle is not considered, since the mMAG would not have the time to send that message before the signal gets weak. In this way, the velocity of the vehicle in the tests is of approximately 25 km/h. The results of this experiment should then show that there is no packet loss derived from the change of the PoAs, and that the handover process was replaced by a process that allows the roaming of one node using the multihoming functionalities. In this situation, the traffic is generated from the CN to the mMAG 1.

- **Multihop:** The second phase of the road experiments depicted in the figure 5.6 aims to show that the multihop feature is perfectly viable and that the vehicle which is connected in multihop can receive traffic also seamlessly when the first hop vehicle changes its PoA. The conditions of this experiment are exactly the same as in the previous one, but in this case the traffic is generated from the CN to the mMAG 2 connected in multihop to the mMAG 1.

5.4 Results

5.4.1 Laboratory scenario

The results of the laboratory testbed will now be presented. These results were obtained as described in 5.3.1, analysed with Microsoft Excel [90] and plotted with MATLAB [91] revision 2013a. All results presented here are a mean of the number of runs with a 95 % confidence level.

5.4.1.1 Overal multihoming performance

First of all, the throughput results are shown in figure 5.7 for different scenarios and traffic rate. They consider scenarios where the same traffic is sent through only one PoA (PoA 1, PoA 2 or PoA 3), through two PoAs (PoA 1/3) and three PoAs (PoA 1/2/3). These results are according with the expected. Here it is visible that the WAVE PoAs (1 and 2) reach indeed approximately the aforementioned 12.9 Mbps, and the Wi-Fi one (PoA 3) reaches indeed the 6.9 Mbps approximately. It is also noticeable in this graph that the multihoming results can withstand all the traffic sent, performing the bandwidth aggregation between the available throughput of both technologies.

Relatively to the packet loss, this information depicted in the figure 5.8 complements the throughput one. It is visible that the 18 Mbps only manage to be transferred when there is multihoming and the bandwidth of both technologies is used. Also, it is visible that the packet loss is very low, almost null, every time that the rate does not surpass the limitations of the interfaces.

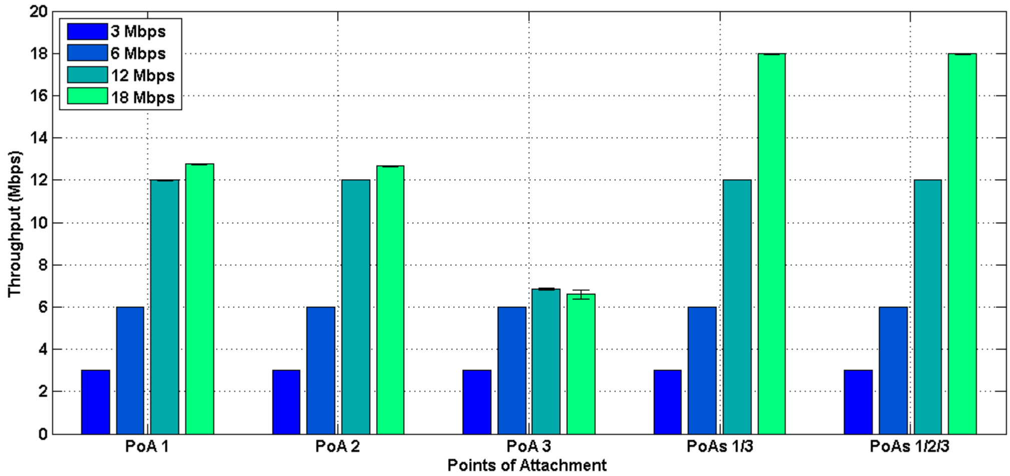


Figure 5.7: Bitrate obtained in the several situations and with variation of traffic

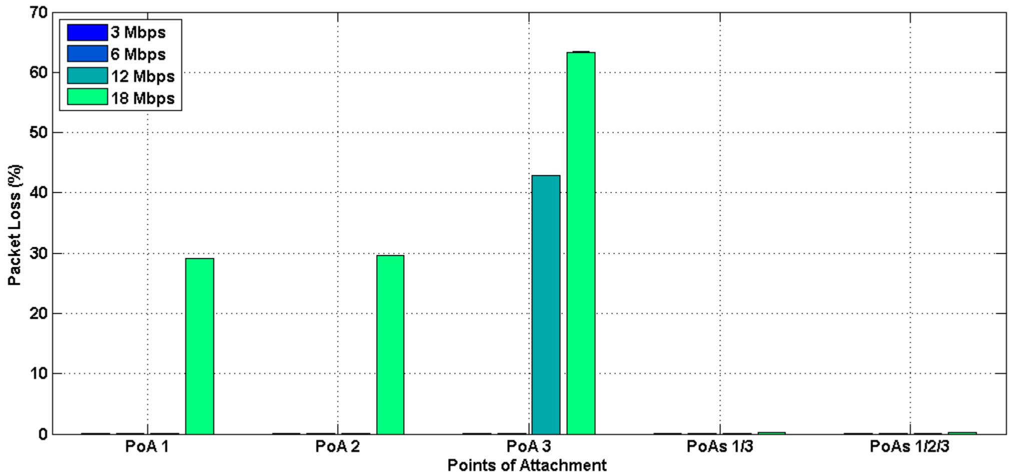


Figure 5.8: Packet loss obtained in the several situations and with variation of traffic

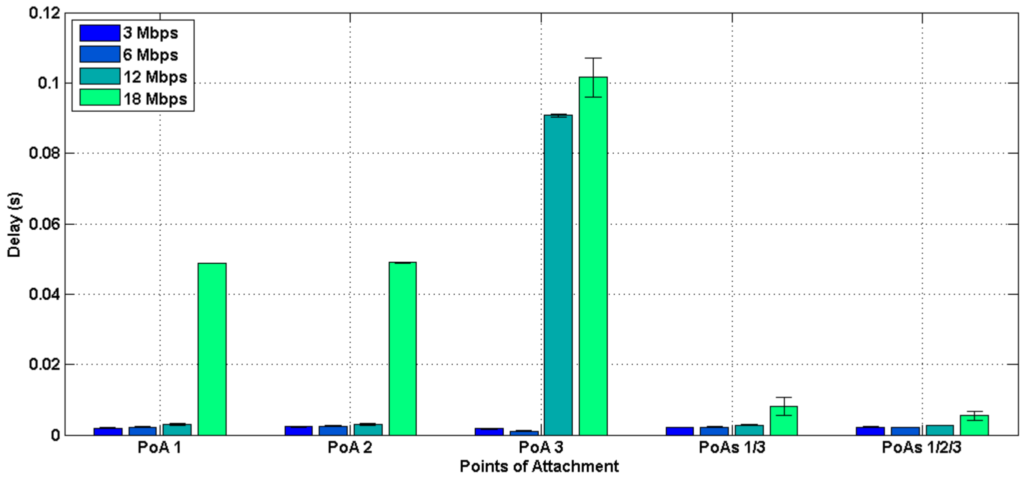


Figure 5.9: Delay obtained in the several situations and with variation of traffic

Regarding the delay in the figure 5.9, it is visible that the multihoming improves the mean time that the packets spend in the network. Also, the situation depicted shows one particularity: the delay of the packets for the 18 Mbps transfer is lower when using three PoAs than when using two. This fact is only verified due to the division of the processing demand for each PoA; otherwise, the usage of only one WAVE PoA could even show better results than using two because of the usage of the same access medium.

Finally, figure 5.10 shows the improvement in the output load of each PoA when the mMAG connects to the three MAGs. Here, only the output load is shown, since the input one depends on the conditions of the network. If the WAVE MAGs see each other, the input load of one MAG will include the output load of the other one. In the other side, the analysis of the results show that the output load of each PoA is lower when using three PoAs, and the load of the WAVE ones will not surpass 50% because the rule is defined to try to not saturate the channel which is divided between those two.

5.4.1.2 Optimized Division Rule

Best division

Figure 5.11 shows the dynamic rule compared with two static ones that differ from the dynamic one in 10% each. As observed, using multihoming through two PoAs (PoA 1 and 3) the dynamic one reaches values around 70% for the WAVE PoA and 30% for the Wi-Fi. These values are registered due to the difference in the capacities, since the WAVE one has a capacity of 12.9 Mbps and the Wi-Fi one has a capacity of 6.9 Mbps. It is visible that the delay results are better for the optimal rule than for the deviations.

Also, the adaptation of the rule is shown in the figure 5.12. This graph starts with no interference and evolves with an increasing extra traffic created by another mMAG that

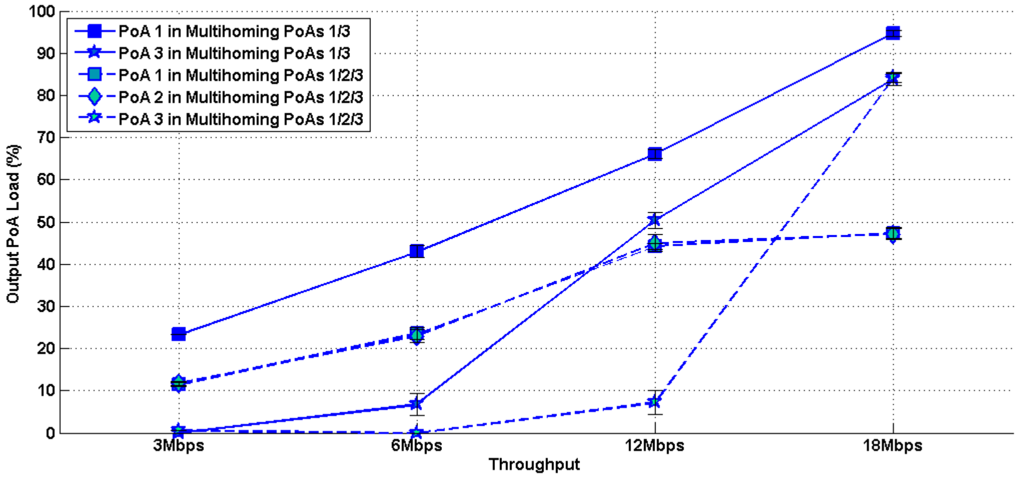


Figure 5.10: Output load of each PoA when in multihoming using two PoAs and three PoAs

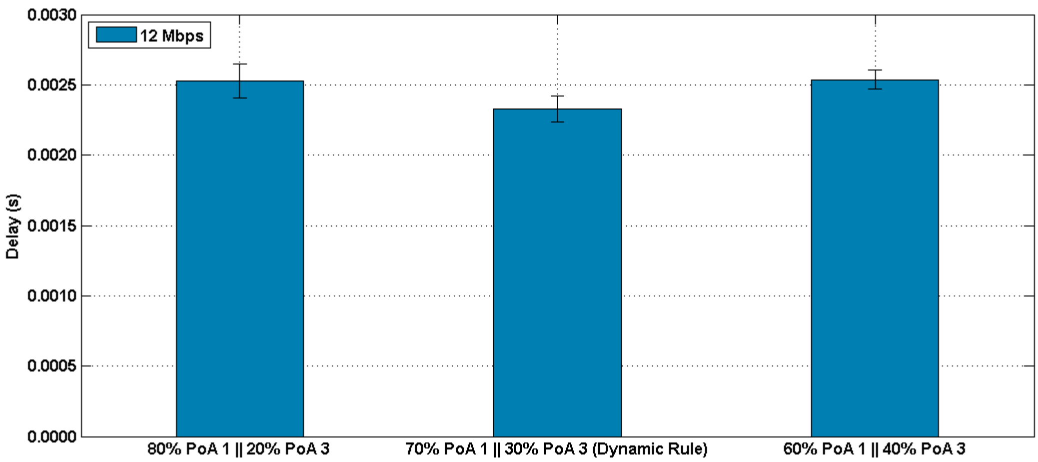


Figure 5.11: Delay comparison between optimal dynamic rule and a static variation of the optimal one

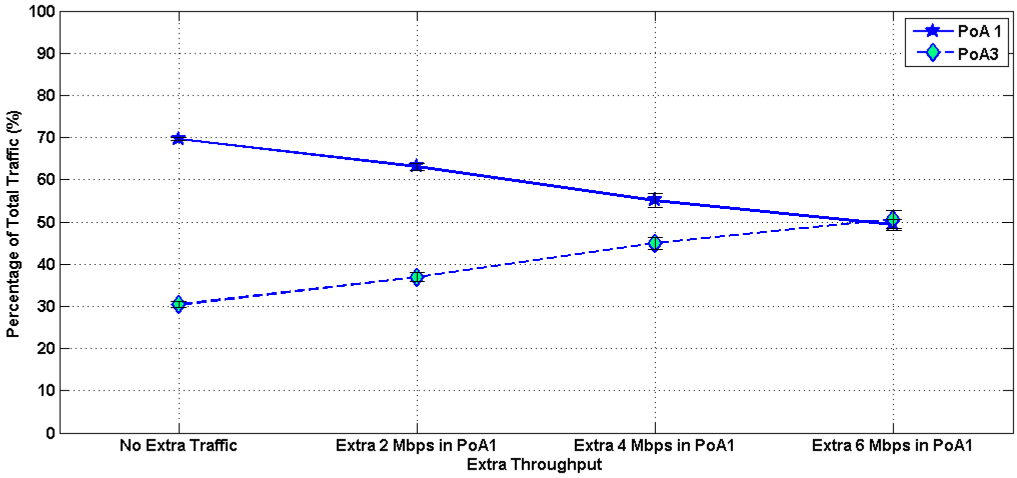


Figure 5.12: Dynamics of the rule when the traffic in one of the interfaces increases

interferes with the WAVE PoA, as depicted in figure 5.4. The first case has the same division as shown in the previous graph, the one that ensures the best delay without any extra traffic. In the consequent measurements with 2, 4 and 6 Mbps, it is visible that the allocated percentage varies accordingly, lowering for the affected PoA and increasing for the other one. The division eventually reaches a value in which the traffic sent for each PoA reaches approximately 50%, which is the value that evens the load. In this last case, the PoA 1 has 6 Mbps plus 50% of 12Mbps, which completes 12 Mbps (its limit is 12.9 Mbps) and the PoA 3 reaches 50% of the sent 12 Mbps (its capacity is 6.9 Mbps).

Group and flow division performance

Figure 5.13 shows the case in which the traffic on one mMAG is treated and divided by the three available MAGs during 10 iterations of the rule calculation. Also, figure 5.14 shows in one of the iterations which are the flows that go through each MAG and to which type they belong. It is visible that the most prioritized traffic (type 2) is sent all through the first network, the second most prioritized is sent through two networks and the least prioritized is divided for all. The analyses of each type of traffic is further explained next:

- **Type 2:** This type of traffic is composed, in this case, of five flows of 1 Mbps each, which completes 5 Mbps. This traffic, being the first to be assigned, easily fits in the first network that has an allocated capacity of 38.2% of the total 16.5 Mbps sent (6.3 Mbps), leaving 1.3 Mbps non-allocated.
- **Type 1:** The second most prioritized type of traffic sends, in this case, five flows of 1.5 Mbps each, comprising a total of 7.5 Mbps. At this point the available throughput comprises 1.3 Mbps in the first network, 6.3 Mbps in the second network (38.1% of the total traffic) and 3.9 Mbps in the third one (23.7% of the total traffic). Hence,

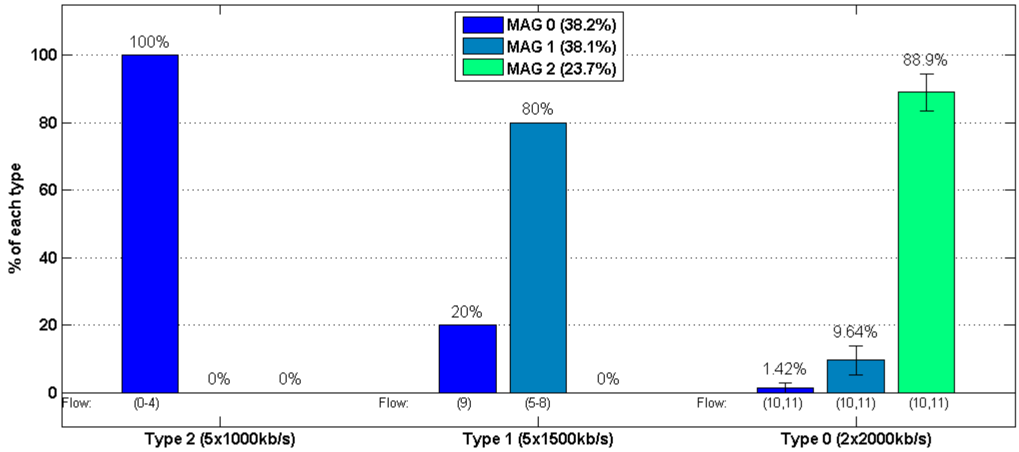


Figure 5.13: Division of each type of traffic by the MAGs when the most prioritized group fits one network and the second is divided by flows

---

as the available throughput in the best network does not fit all the flows of this type, four of them are allocated to MAG 1 and the other one is allocated to the other WAVE network. As seen in the figure 5.14, although the 1.5 Mbps surpass the available percentage in this network, it does not surpass the total capacity of the MAG, then, as the total throughput will not surpass the limit mentioned, set to 10% of the allocated 38.2% which is 3.82%, the flow is allocated to the first network (it only surpasses in 1.2%). This extra percentage allocated to the WAVE network is then discounted in the other networks.

- **Type 0:** Finally, the allocated of the least prioritized type of traffic is done through the algorithm of packet distribution used in the previous implementation of multi-homing and uses the still available percentages in each network. It is visible that some of the traffic of this type is routed through the first network sometimes. This is due to the possible variations in the packets sent, control messages and readings in each MAG. Also, most of the traffic of this type is routed through the MAG 2 and some of it is routed through the MAG 1, which is due to the fact that the rest of the bandwidth defined by the genetic algorithm is already occupied by the other traffic types that have a higher priority.

Resuming, as it is visible in the figure 5.14 relating to one of the iterations of the rule calculation, the type 2 flows (from 0 to 4) are sent all through the MAG 0, four of the type 1 flows (from 5 to 8) are sent through the MAG 1 and the other one (flow 9) fills the attributed percentage to the first MAG surpassing a little so that the flow is not divided, and finally the type 0 flows (10 and 11) go mostly through the last MAG (the Wi-Fi one) and a little bit in through the MAG 1. Notice that, in some iterations, the variability of the messages exchanged take the algorithm to allocate a part of the type 0 traffic to the

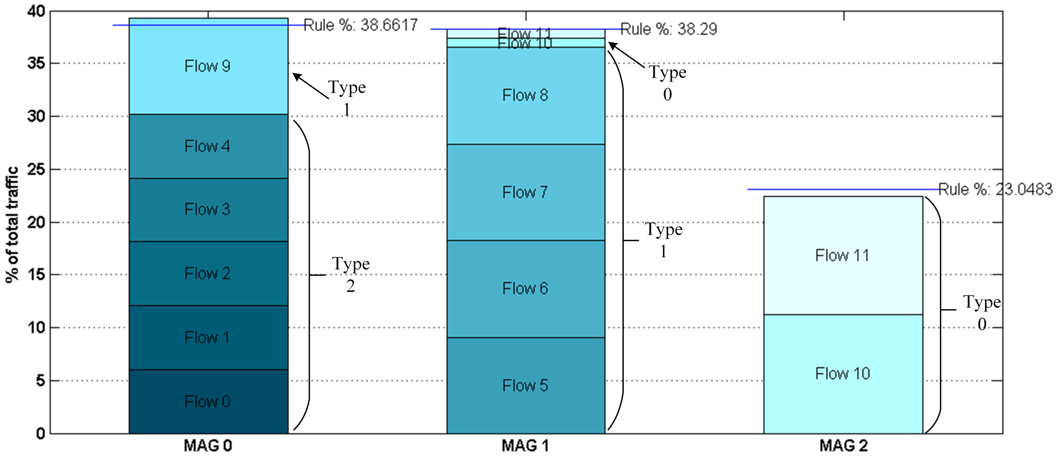


Figure 5.14: Flows that go through each MAG when type 2 fits entirely in one network and type 1 is divided through two networks per flow

---

first MAG when the flows 0 to 4 and 9 do not fill entirely its allocated percentage.

Figure 5.15 shows the main improvement brought by the distribution of the flows and groups by the available networks based on its priority. One of the problems of the previous implementation [7] was that, with the different delay of several paths, the packets of one flow reached the destination out of its original order. The results of the out-of-order packets are shown: they reach approximately 0.13% in this laboratory scenario in which the differences of delay between the paths is not high. With the improvement of this distribution, the out-of-order packets lower significantly. For the best priorities of traffic, the value is almost zero and it just registers some of these packets during the time of the first calculation because it changes the place to which they are being sent. In the case of the least prioritized type, although the flow distribution is not performed, the out-of-order packets are also lowered because the packets of this group are mostly routed through the same network which is the one that is not being allocated to the other types of traffic.

Time expenditure

The time of calculation of the rule is also very important in the vehicular networks. The figure 5.16 shows the time it takes to perform each task, being the most costly processes the information requests to the MAGs and the genetic algorithm execution. Relatively to the information requests, the LMA requests the information and has to wait for the response of each MAG before it follows to the calculations, which may take some time. Relatively to the genetic algorithm calculation, each time it is used, it has to start a generation and follow with genetic procces as described. Moreover, relatively to the added block of the flows assignment, the time it takes to calculate is almost insignificant when related to the rest of the times.

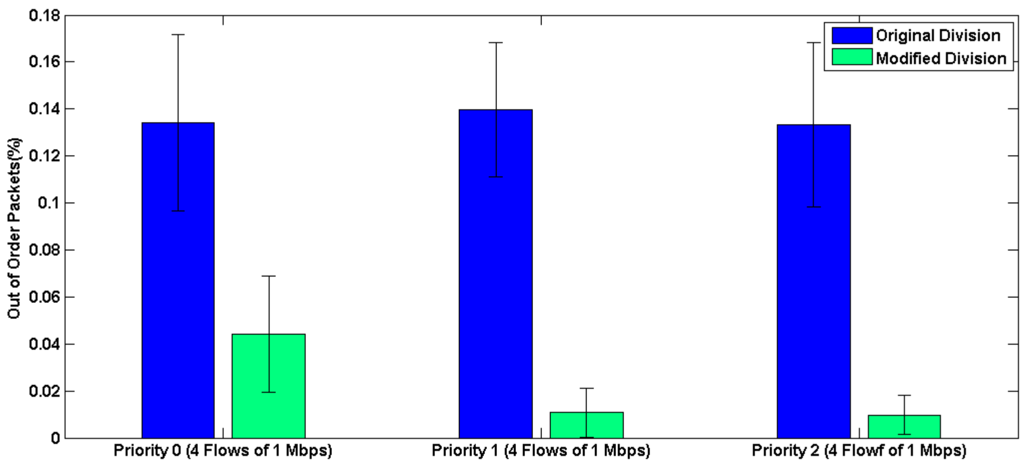


Figure 5.15: Out of order packets in the first implementation compared with the improved version

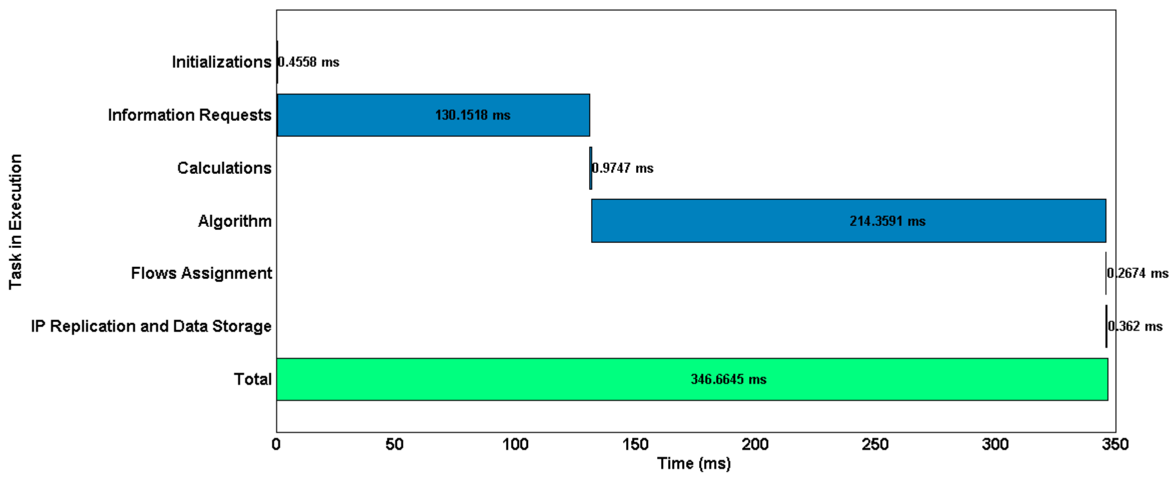


Figure 5.16: Time expenditure during the calculation of the division rule

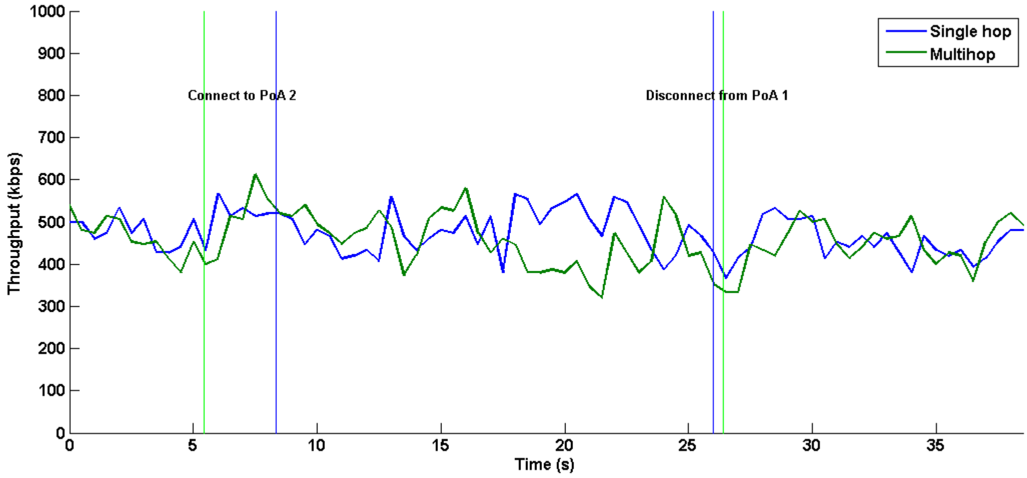


Figure 5.17: Throughput obtained during the trip of the vehicle in single hop compared with multihop

5.4.2 Road Scenario

The throughput obtained during this experiment is shown in the figure 5.17 with a sampling interval of 500 ms. This result shows average values of three experiments of each test, and shows that there are no losses while the vehicle travels and changes the PoA: first it is connected to PoA 1, then to both PoAs with a 50% rule, since the network conditions are the same, and finally to only PoA 2. In the multi-hop scenario mMAG2 travels near mMAG1 and connects to the infrastructure through mMAG1.

Also, it is visible that neither the single-hop scenario neither the multihop one show any increased losses at the time of the connection to the PoA 2 (starting a multihoming situation with the two connections simultaneously) neither at the time of the disconnection from the PoA 1 (when the multihoming process attributes all the traffic to the PoA 2 due to the reception of the disconnect message). The variations seen in the throughput can be explained by some factors: the different delays of some packets, since on one side, they may travel through different paths, and on the other side, there are interferences in the Wi-Fi connections LMA - MAGs; the velocity that can affect the time in which the packet arrives to the mMAG; and the differences in the several parts of the scenarios, namely the relative position of each node, the reflections and the obstructions of visibility during the tests.

This result shows that the implementation of the message that aims to inform the LMA about the disconnection of the mMAG from one MAG is functional. The rule is recalculated when it should, and the LMA only sends traffic to the MAGs that need to receive it.

It is also visible that the difference between the single-hop connection and the multihop connection is not significant, since although there is one more hop, the medium is not saturated and the messages can be transmitted and received without problems in both mMAGs.

Finally, this experiment demonstrates that the integration of the solution described in this dissertation with the mentioned parallel dissertation is capable of providing multihoming combining the functionalities that were worked upon the two dissertations mentioned in the section 3.6.

5.5 Chapter considerations

The laboratory and road scenarios allow the verification of the functionalities of the multihoming implementation in VANETs. With the laboratory results, it becomes visible that the multihoming is capable to improve the conditions of the service improving the delay, throughput and packet loss when relating to the solution with just one interface.

Also, it is proven that the solution implements a dynamic traffic distribution rule capable of minimizing the delay and maximizing the utilization of WAVE. The output load of the PoAs is also a factor that is improved by the solution, in the way that each MAG has less packets to process than in the one connection case. Moreover, this rule is capable of providing an adaptation to the extra traffic introduced by other users in the MAGs with even loads.

The classification of the traffic and the interfaces allow the better utilization of the allocated rule for each path and, in this way, the same rule can fulfill better performance minimizing the division of each flow. Therefore, the correct allocation of the higher priority flows shows its importance through the minimization of the out-of-order packets. This minimization may bring advantages in the utilization of both UDP and TCP traffic, since in the UDP, the less out-of order packets will improve the performance of the applications, and in the TCP this minimization will allow the transmission window to be larger (since the out-of-order packets may be accounted as losses consequently lowering this window).

Relatively to the time of calculation of the rule, this is not high which allows a good utilization of the solution in the dynamic environment of the VANETs.

Finally, the road experiments show that the solution can accomplish a good performance in the way that it does not loose packets when it travels from a point where it is connected to one MAG to another point where it is connected to two, and to another point where it disconnects from the first one. This factor allows one vehicle to roam without the need to perform a handover, since it can connect to two PoAs as a transition phase instead of the traditional handover mechanism, in which it has to disconnect from one and connect to the other one.

These evaluations allow to verify the proper functioning of the implemented solution and that the proposed objectives are accomplished. The several features that were worked upon this dissertation and the merged features in the integration with the other dissertation are working well, and their evaluation shows that they actually bring advantages to the performance of the overall solution.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

This dissertation had the aim to study the actual state of the mobility and multihoming protocols and their use on a vehicular scenario. Moreover, it was also the objective to implement a mobility and multihoming solution taking into account the requirements of a vehicular scenario when in the operation of this solution.

To this implementation a vehicular mobility solution based on N-PMIPv6 was used and integrated with a multihoming extension for PMIPv6. This solution was also integrated in real OBUs and RSUs in the way that some adjustments were made.

Upon the integration, in order to enable the mMAG to connect to different PoAs, an enhanced connection manager that supports multihoming was developed. This connection manager takes into account another feature implemented in this work: the connection to different PoAs with just one WAVE interface. This other feature added to our solution allows the multihoming to be more effective without adding more interfaces to the OBU. This change was also worked upon the LMA.

Besides, another fulfilled objective was the adaptation of the traffic distribution rule to the VANET reality. This change allowed the distribution to be performed in a more correct manner to the vehicular environment through the qualitative classification of the traffic and the networks.

The evaluation of the work developed included laboratory and road scenarios and tested different aspects of the solution, which allowed the analysis of the obtained results, and several conclusions to be taken:

- The multihoming is functional and fulfils its objectives, managing to distribute the traffic by the different interfaces maximizing the utilization of the vehicular technology (WAVE), minimizing the time that the packets spend in the network and increasing the total throughput that one vehicle can reach.

- The implementation of the multihoming using just one interface allows to decrease the output load of each MAG and also lower its processing needs.

- Besides the calculation of the best way to distribute the traffic, the dynamic rule can adapt to changes in the extra traffic that does not belong to that user, performing load balancing.

- The classification of the networks according to their characteristics allows the traffic to be distributed accordingly.

- The classification of the traffic according to its priority allows the LMA to relate this information with the networks classification and send the more important traffic through the best networks.

- Through the allocation of the whole flow to one network, the performance of the solution is improved in the way that the vehicle receives much less out-of-order packets.

- Regarding the timings, the calculation of the rule is not too costly allowing the solution to perform in a dynamic environment.

- Multihoming can provide the vehicle with mobility apart from the traditional handover scenario, without loosing packets.

- The integrated solution with the parallel dissertation is able to provide multihoming with multihop and also take advantage of the dynamic traffic distribution rule.

With these results we can conclude that, although there are still improvements to be made to the solution, it can already perform multihoming in a real vehicular network, with support for mobility, multihop and a dynamic rule capable of providing an improved service.

6.2 Future Work

With the development of this dissertation, there are several aspects within this solution that may be improved in order to obtain a better approach. These improvements are:

- **Identification of the traffic types:** The actual manner of identification of the type of traffic is through the simple analysis of its port, being three ports allocated to three different priorities. The implementation of an algorithm that analyses and identifies the traffic would allow the integration of this feature with a wider range of applications, namely real internet traffic, information logs, sensors traffic, infotainment contents and much more.

- **Improved disconnect message:** One of the main aspects that may largely improve de disconnection process is the transmission of a disconnect message through a good link whenever one interface is disconnecting. This message is actually being sent through the same PoA that is disconnecting, but an improved approach should identify the interface and the serving MAG from which it is disconnecting and send the message through a good quality link.

- **Packet reordering:** When the packets reach its destination, if they are getting there through different paths, some of them will arrive in a different order than it is supposed. In this way, a packet reordering algorithm is needed to improve the performance of multihoming.

- **Uplink multihoming:** in the actual version of this solution, only the downlink traffic is treated and divided in the multihoming process. A good improvement would be the implementation of a uplink multihoming process that would allow the division of the traffic through the several connections when uploading files. With this implementation, the managing of the uplink default rule in the connection manager would be unnecessary.

- **Overhead of the network:** With the tunnel utilization to connect the LMA to the MAGs or mMAGs, the overhead is highly increased, specially when in multihop where one tunnel goes within the previous one. A lighter solution should be used.

- **Scalability:** The operation of the LMA takes a lot of processing that can be too heavy to a normal computer when the network is bigger. In this way, the LMA should be implemented in a computer with high capacity for processing all the information of a relatively bigger network. Also, an improvement would be the utilization of several LMAs that would allow a more distributed approach.

- **Network coding:** The implementation of network coding allows a better transmission of the messages through more than one path and also solves the problem of the packet reordering.

Bibliography

[1] I. S. Association *et al.*, "802.11 p-2010—ieee standard for information technology—local and metropolitan area networks—specific requirements—part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments," *URL http://standards. ieee. org/findstds/standard/802.11 p-2010. html*.

[2] J. Dias, A. Cardote, F. Neves, S. Sargento, and A. Oliveira, "Seamless horizontal and vertical mobility in vanet," in *Vehicular Networking Conference (VNC), 2012 IEEE*. IEEE, 2012, pp. 226–233.

[3] J. F. Dias, "Mobilidade em comunicações veiculares," Master's thesis, Universidade de Aveiro, 2010.

[4] D. M. A. Lopes, "Acesso à internet com handover de veículos através de gateways móveis," 2013.

[5] J. P. C. Azevedo, "Wireless distributed mobility management on a road scenario," Master's thesis, Universidade de Aveiro, 2014.

[6] F. C. O. d. A. Martins, "Separação de identificação e localização para mobilidade de veículos," Master's thesis, Universidade de Aveiro, 2014.

[7] N. Capela and S. Sargento, "An intelligent and optimized multihoming approach in real and heterogeneous environments," *Wireless Networks*, pp. 1–21.

[8] C2C-CC. Car 2 car comunication consortium. [Online]. Available: https://www.car-2-car.org/index.php?id=5

[9] R. Uzcategui and G. Acosta-Marum, "Wave: a tutorial," *Communications Magazine, IEEE*, vol. 47, no. 5, pp. 126–133, 2009.

[10] "Ieee 802.11 wireless local area networks," grouper.ieee.org/groups/802/11/, accessed: 2015-08-10.

[11] ETSI. (2013-05) draft etsi en 302 571 v1.2.0. "intelligent transport systems (its); radiocommunications equipment operating in the 5855 mhz to 5925 mhz frequency band; harmonized en covering the essential requirements of article 3.2 of the r&tte

directive". [Online]. Available: http://www.etsi.org/deliver/etsi_en/302500_302599/302571/01.02.00_20/en_302571v010200a.pdf

[12] "Trial-use standard for wireless access in vehicular environments (wave) - resource manager," *IEEE Std 1609.1-2006*, pp. 1–71, Oct 2006.

[13] "Trial-use standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Std 1609.2-2006*, pp. 1–116, July 2006.

[14] "Ieee trial-use standard for wireless access in vehicular environments (wave) - networking services," *IEEE Std 1609.3-2007*, pp. 1–99, April 2007.

[15] "Ieee trial-use standard for wireless access in vehicular environments (wave) - multichannel operation," *IEEE Std 1609.4-2006*, pp. 1–82, Nov 2006.

[16] M. Nekovee, "Sensor networks on the road: the promises and challenges of vehicular adhoc networks and vehicular grids," in *Proceedings of the Workshop on Ubiquitous Computing and e-Research*, 2005.

[17] M. Tsukada, J. Santa, S. Matsuura, T. Ernst, and K. Fujikawa, "On the experimental evaluation of vehicular networks: Issues, requirements and methodology applied to a real use case," *arXiv preprint arXiv:1504.04426*, 2015.

[18] H. Moustafa and Y. Zhang, *Vehicular networks: techniques, standards, and applications.* Auerbach publications, 2009.

[19] "iperf - the network bandwidth measurement tool," https://iperf.fr/, accessed: 2015-08-10.

[20] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 4, pp. 584–616, 2011.

[21] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *Communications Magazine, IEEE*, vol. 47, no. 11, pp. 84–95, 2009.

[22] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 ghz dsrc-based vehicular safety communication," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 36–43, 2006.

[23] W. Xiang, P. Richardson, and J. Guo, "Introduction and preliminary experimental results of wireless access for vehicular environments (wave) systems," in *Mobile and Ubiquitous Systems-Workshops, 2006. 3rd Annual International Conference on.* IEEE, 2006, pp. 1–8.

[24] Y. L. Morgan, "Notes on dsrc & wave standards suite: Its architecture, design, and characteristics," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 4, pp. 504–518, 2010.

[25] L. Miao, K. Djouani, B. J. van Wyk, and Y. Hamam, "Evaluation and enhancement of ieee 802.11 p standard: A survey," *Mobile Computing*, vol. 1, no. 1, 2012.

[26] S. Gräfling, P. Mahonen, and J. Riihijarvi, "Performance evaluation of ieee 1609 wave and ieee 802.11 p for vehicular communications," in *Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on.* IEEE, 2010, pp. 344–348.

[27] D. Jiang and L. Delgrossi, "Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE.* IEEE, 2008, pp. 2036–2040.

[28] Y. Du, L. Zhang, Y. Feng, Z. Ren, and Z. Wang, "Performance analysis and enhancement of ieee 802.11 p/1609 protocol family in vehicular environments," in *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on.* IEEE, 2010, pp. 1085–1090.

[29] C. Wewetzer, M. Caliskan, K. Meier, and A. Luebke, "Experimental evaluation of umts and wireless lan for inter-vehicle communication," in *Telecommunications, 2007. ITST'07. 7th International Conference on ITS.* IEEE, 2007, pp. 1–6.

[30] A. Vinel, "3gpp lte versus ieee 802.11 p/wave: which technology is able to support cooperative vehicular safety applications?" *Wireless Communications Letters, IEEE*, vol. 1, no. 2, pp. 125–128, 2012.

[31] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "Lte for vehicular networking: a survey," *Communications Magazine, IEEE*, vol. 51, no. 5, pp. 148–157, 2013.

[32] G. R. Hiertz, D. Denteneer, P. L. Stibor, Y. Zang, X. P. Costa, and B. Walke, "The ieee 802.11 universe," *Communications Magazine, IEEE*, vol. 48, no. 1, pp. 62–70, 2010.

[33] J. Jansons, E. Petersons, and N. Bogdanovs, "Vehicle-to-infrastructure communication based on 802.11 n wireless local area network technology," in *Future Internet Communications (BCFIC), 2012 2nd Baltic Congress on.* IEEE, 2012, pp. 26–31.

[34] H. Menouar, F. Filali, and M. Lenardi, "A survey and qualitative analysis of mac protocols for vehicular ad hoc networks," *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 30–35, 2006.

[35] H. Hartenstein and K. Laberteaux, *VANET vehicular applications and inter-networking technologies.* John Wiley & Sons, 2009, vol. 1.

[36] C2C-CC. (2007) Car 2 car communication consortium manifesto: Overview of the c2c-cc system. [Online]. Available: https://www.car-2-car.org/index.php?eID=tx_nawsecuredl&u=0&g=0&t=1444861682&hash=bae702d6648e5eb4a722150951d0bcbaec5fff5a&file=fileadmin/downloads/C2C-CC_manifesto_v1.1.pdfhttp://www.etsi.org/deliver/etsi_en/302500_302599/302571/01.02.00_20/en_302571v010200a.pdf

[37] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. In Kim, "Mobility and handoff management in vehicular networks: a survey," *Wireless communications and mobile computing*, vol. 11, no. 4, pp. 459–476, 2011.

[38] D. Le, X. Fu, D. Hogrefe *et al.*, "A review of mobility support paradigms for the internet." *IEEE Communications Surveys and Tutorials*, vol. 8, no. 1-4, pp. 38–51, 2006.

[39] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6," RFC 6275 (Proposed Standard), Internet Engineering Task Force, Jul. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6275.txt

[40] C. Perkins, "IP Mobility Support for IPv4, Revised," RFC 5944 (Proposed Standard), Internet Engineering Task Force, Nov. 2010. [Online]. Available: http://www.ietf.org/rfc/rfc5944.txt

[41] D. A. Joseph, "Mobility support in ipv6."

[42] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963 (Proposed Standard), Internet Engineering Task Force, Jan. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc3963.txt

[43] H.-N. Nguyen and C. Bonnet, "An intelligent tunneling framework for always best connected support in network mobility (nemo)," in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE.* IEEE, 2008, pp. 3021–3026.

[44] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213 (Proposed Standard), Internet Engineering Task Force, Aug. 2008, updated by RFC 6543. [Online]. Available: http://www.ietf.org/rfc/rfc5213.txt

[45] A. Udugama, M. U. Iqbal, U. Toseef, C. Goerg, C. Fan, and M. Schlaeger, "Evaluation of a network based mobility management protocol: Pmipv6," in *Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th.* IEEE, 2009, pp. 1–5.

[46] S. Jeon, B. Sarikaya, and R. Aguiar, "Network mobility support using mobile mag in proxy mobile ipv6 domain," Working Draft, IETF Secretariat, Internet-Draft draft-sijeon-netext-mmag-pmip-00, October 2012, http://www.ietf.org/internet-drafts/draft-sijeon-netext-mmag-pmip-00.txt. [Online]. Available: http://www.ietf.org/internet-drafts/draft-sijeon-netext-mmag-pmip-00.txt

[47] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The Locator/ID Separation Protocol (LISP)," RFC 6830 (Experimental), Internet Engineering Task Force, Jan. 2013. [Online]. Available: http://www.ietf.org/rfc/rfc6830.txt

[48] T. Condeixa and S. Sargento, "Dynamic mobile ip anchoring," in *Communications (ICC), 2013 IEEE International Conference on*. IEEE, 2013, pp. 3607–3612.

[49] J. Azevedo, T. Condeixa, and S. Sargento, "Distributed ip mobility in a real vehicular network," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2419–2424.

[50] F. Teraoka and T. Arita, "Pnemo: a network-based localized mobility management protocol for mobile networks," in *Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on*. IEEE, 2011, pp. 168–173.

[51] H. Naderi and B. E. Carpenter, "A review of ipv6 multihoming solutions," in *Tenth International Conference on Networks (ICN 2011)*, 2011, pp. 145–150.

[52] P. Mitharwal, C. Lohr, and A. Gravey, "Survey on network interface selection in multihomed mobile networks," in *Advances in Communication Networking*. Springer, 2014, pp. 134–146.

[53] J. Bi, P. Hu, and L. Xie, "Site multihoming: Practices, mechanisms and perspective," in *Future Generation Communication and Networking (FGCN 2007)*, vol. 1. IEEE, 2007, pp. 535–540.

[54] B. M. Sousa, K. Pentikousis, and M. Curado, "Multihoming management for future networks," *Mobile Networks and Applications*, vol. 16, no. 4, pp. 505–517, 2011.

[55] A. L. Ramaboli, O. E. Falowo, and A. H. Chan, "Bandwidth aggregation in heterogeneous wireless networks: A survey of current approaches and issues," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1674–1690, 2012.

[56] K. Habak, K. A. Harras, and M. Youssef, "Bandwidth aggregation techniques in heterogeneous multi-homed devices: A survey," *arXiv preprint arXiv:1309.0542*, 2013.

[57] A. Gladisch, R. Daher, and D. Tavangarian, "Survey on mobility and multihoming in future internet," *Wireless personal communications*, vol. 74, no. 1, pp. 45–81, 2014.

[58] R. Stewart, "Stream Control Transmission Protocol," RFC 4960 (Proposed Standard), Internet Engineering Task Force, Sep. 2007, updated by RFCs 6096, 6335, 7053. [Online]. Available: http://www.ietf.org/rfc/rfc4960.txt

[59] R. Ferrús, A. Brunstrom, K.-J. Grinnemo, R. Fracchia, G. Galante, F. Casadevall *et al.*, "Towards transport-layer mobility: Evolution of sctp multihoming," *Computer Communications*, vol. 31, no. 5, pp. 980–998, 2008.

[60] T. D. Wallace and A. Shami, “A review of multihoming issues using the stream control transmission protocol,” *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 2, pp. 565–578, 2012.

[61] A. Ford, C. Raiciu, M. Handley, S. Barre, and J. Iyengar, “Architectural Guidelines for Multipath TCP Development,” RFC 6182 (Informational), Internet Engineering Task Force, Mar. 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6182.txt

[62] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, “TCP Extensions for Multipath Operation with Multiple Addresses,” RFC 6824 (Experimental), Internet Engineering Task Force, Jan. 2013. [Online]. Available: http://www.ietf.org/rfc/rfc6824.txt

[63] R. Moskowitz, T. Heer, P. Jokela, and T. Henderson, “Host Identity Protocol Version 2 (HIPv2),” RFC 7401 (Proposed Standard), Internet Engineering Task Force, Apr. 2015. [Online]. Available: http://www.ietf.org/rfc/rfc7401.txt

[64] J. Laganier and F. Dupont, “An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2),” RFC 7343 (Proposed Standard), Internet Engineering Task Force, Sep. 2014. [Online]. Available: http://www.ietf.org/rfc/rfc7343.txt

[65] E. Nordmark and M. Bagnulo, “Shim6: Level 3 Multihoming Shim Protocol for IPv6,” RFC 5533 (Proposed Standard), Internet Engineering Task Force, Jun. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5533.txt

[66] A. García-Martínez, M. Bagnulo, and I. Van Beijnum, “The shim6 architecture for ipv6 multihoming,” *Communications Magazine, IEEE*, vol. 48, no. 9, pp. 152–157, 2010.

[67] O. EURECOM. Openairinterface proxy mobile ipv6 (oai pmipv6). [Online]. Available: http://openairinterface.eurecom.fr/openairinterface-proxy-mobile-ipv6-oai-pmipv6

[68] UMIP. Umip - mobile ipv6 and nemo for linux). [Online]. Available: http://umip.org/

[69] J. Murai *et al.* Usagi project - linux ipv6 development project). [Online]. Available: http://www.linux-ipv6.org/

[70] D. M. A. Lopes, “Acesso à internet com handover de veículos através de gateways móveis,” Master’s thesis, Universidade de Aveiro, 2013.

[71] J. Chu and V. Kashyap, “Transmission of IP over InfiniBand (IPoIB),” RFC 4391 (Proposed Standard), Internet Engineering Task Force, Apr. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4391.txt

[72] N. Capela and S. Sargento, “Multihoming and network coding: A new approach to optimize the network performance,” *Computer Networks*, vol. 75, pp. 18–36, 2014.

[73] M. Li, M. Claypool, and R. Kinicki, "Wbest: A bandwidth estimation tool for ieee 802.11 wireless networks," in *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on.* IEEE, 2008, pp. 374–381.

[74] Openwrt wireless freedom. [Online]. Available: https://openwrt.org/

[75] Buildroot: Making embedded linux easy. [Online]. Available: http://buildroot.uclibc.org/

[76] Barrier breaker. [Online]. Available: http://wiki.openwrt.org/doc/barrier.breaker

[77] Openwrt build system – installation. [Online]. Available: http://wiki.openwrt.org/doc/howto/buildroot.exigence

[78] M. Becker. Openwrt buildroot. [Online]. Available: https://downloads.openwrt.org/docs/buildroot-documentation.html#about

[79] An introduction to buildroot-ng. [Online]. Available: https://forum.openwrt.org/viewtopic.php?pid=31794#p31794

[80] Creating packages. [Online]. Available: http://wiki.openwrt.org/doc/devel/packages

[81] The freeradius client library. [Online]. Available: http://freeradius.org/freeradius-client/

[82] Ndisc6 : Ipv6 diagnostic tools for linux and bsd. [Online]. Available: http://www.remlab.net/ndisc6/

[83] Tcpdump & libpcap. [Online]. Available: http://www.tcpdump.org/

[84] The netfilter.org "libnetfilter_queue" project. [Online]. Available: http://www.netfilter.org/projects/libnetfilter_queue/

[85] The freeradius project. [Online]. Available: http://freeradius.org/

[86] Linux wireless - about iw. [Online]. Available: http://linuxwireless.org/en/users/Documentation/iw/__v33.html

[87] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861 (Draft Standard), Internet Engineering Task Force, Sep. 2007, updated by RFCs 5942, 6980, 7048, 7527, 7559. [Online]. Available: http://www.ietf.org/rfc/rfc4861.txt

[88] C. Ameixieira, A. Cardote, F. Neves, R. Meireles, S. Sargento, L. Coelho, J. Afonso, B. Areias, E. Mota, R. Costa *et al.*, "Harbornet: A real-world testbed for vehicular networks," *Communications Magazine, IEEE*, vol. 52, no. 9, pp. 108–114, 2014.

[89] D-itg, distributed internet traffic generator. [Online]. Available: http://traffic.comics.unina.it/software/ITG/

[90] Excel. [Online]. Available: https://products.office.com/en/excel

[91] Matlab. [Online]. Available: http://www.mathworks.com/products/matlab/